JOURNAL OF ALGEBRA 131, 303–341 (1990)

Finite Groups of Genus Zero*

ROBERT M. GURALNICK

Department of Mathematics,
University of Southern California,
Los Angeles, California 90089–1113

AND

JOHN G. THOMPSON

Department of Pure Mathematics,
University of Cambridge,
Cambridge CB2 1SB, England

Received February 7, 1989

DEDICATED TO WALTER FEIT ON THE OCCASION OF HIS 60TH BIRTHDAY

1. INTRODUCTION

If ϕ is a nonconstant meromorphic function on the compact connected Riemann surface X, we denote by $\mathrm{Mon}(X, \phi)$ the monodromy group of the cover

$$X \xrightarrow{\phi} \mathbb{P}^1. \tag{1}$$

Set

$$\mathscr{S}(X) = \bigcup_{\phi} \mathrm{cf}(\mathrm{Mon}(X, \phi)),$$

where cf (G) denotes the set of composition factors of the group G, and ϕ ranges over all the non-constant meromorphic functions on X. It is well known and elementary that for all X, all primes p, and all $n \geqslant 5$,

$$C_p \in \mathscr{S}(X), \qquad A_n \in \mathscr{S}(X),$$

where C_p is the group of order p and A_n is the alternating group of degree n. Indeed, for each G which is either a C_p or an A_n, there is a cover

$$\mathbb{P}^1 \xrightarrow{\psi} \mathbb{P}^1, \tag{2}$$

* Supported by NSF Grants DMS 8700961 and DMS-8702150.

0021-8693/90 $3.00

depending on G, such that $\mathrm{Mon}(\mathbb{P}^1, \psi) \cong G$, and the composition of (1) and (2) gives us $G \in \mathrm{cf}(\mathrm{Mon}(X, \psi\phi))$. This remarks shows incidentally that

$$\mathscr{S}(\mathbb{P}^1) \subseteq \mathscr{S}(X) \tag{3}$$

for all X. That being so, we are led to define

$$\mathscr{S}^*(X) = \{S \in \mathscr{S}(X) \mid S \text{ is neither cyclic nor alternating}\},$$

and to set, for each family $\mathscr{M}$ of compact connected Riemann surfaces,

$$\mathscr{S}^*(\mathscr{M}) = \bigcup_{X \in \mathscr{M}} \mathscr{S}^*(X).$$

If g is an integer $\geqslant 0$, and $\mathscr{M}_g$ is the family of all compact connected Riemann surfaces of genus g, we set

$$\mathscr{S}^*(\mathscr{M}_g) = \mathscr{E}(g),$$

and call $\mathscr{E}(g)$ the g-exceptional set of simple groups. It seems reasonable to conjecture $\mathscr{E}(g)$ is a finite set for each $g \geqslant 0$, and this paper is a contribution toward a proof that $\mathscr{E}(0)$ is finite. In view of (3), $\mathscr{E}(0)$ plays a special role in the study of $\mathscr{E}(g)$.

Our attack on $\mathscr{E}(0)$ is organized around the classification theorem for finite simple groups, together with the following theorem of Aschbacher and Scott [AS]:

Suppose G is a finite group and H is a maximal subgroup of G such that

$$\bigcap_{g \in G} H^g = 1.$$

Let Q be a minimal normal subgroup of G, let L be a minimal normal subgroup of Q, and let $\Delta = \{L = L_1, L_2, \ldots, L_t\}$ be the set of G-conjugates of L. Then $G = HQ$ and precisely one of the following holds:

(A) L is of prime order p.

(B) $F^*(G) = Q \times R$, where $Q \cong R$ and $H \cap Q = 1$.

(C1) $F^*(G) = Q$ is nonabelian, $H \cap Q = 1$,

(C2) $F^*(G) = Q$ is nonabelian, $H \cap Q \neq 1 = H \cap L$.

(C3) $F^*(G) = Q$ and $H \cap Q = H_1 \times \cdots \times H_t$, where $H_i = H \cap L_i \neq 1$, $1 \leqslant i \leqslant t$.

Let G be a group acting on a finite set Ω. If $x \in G$, define the index of x by

$$\mathrm{ind}\, x = |\Omega| - \mathrm{orb}\, x,$$

where orb x is the number of orbits of $\langle x \rangle$ on Ω.

The dictionary which translates (1) to a group theoretic configuration is well thumbed. The topological nature of X is uniquely determined by the genus $g=g(X)$ of X. From ϕ, we extract a natural number $n=[\mathbb{C}(X):\mathbb{C}(\phi)]$, where $\mathbb{C}(X)$ is the field of meromorphic functions on X, and we get a finite subset S of $\mathbb{P}^1$:

$$S=\{x\in\mathbb{P}^1 \mid |\phi^{-1}(x)|<n\}.$$

If $S=\varnothing$, then $n=1$ and Mon $(X,\phi)=\{1\}$, a case we exclude from further consideration. Let $r=|S|$. Since ϕ is surjective, we get $n>1$. Choose $p_0\in\mathbb{P}^1-S$ and a homotopy basis $\{\gamma_1,\ldots,\gamma_r\}$ for $\pi_1=\pi_1(\mathbb{P}^1-S;p_0)$. Let $\phi^{-1}(p_0)=\{q_1,\ldots,q_n\}$. If γ in π_1 is the homotopy class of the map $f\colon[0,1]\to\mathbb{P}^1-S$, we get an element of S_n associated to γ by lifting f to $f_i\colon[0,1]\to X$, $f_i(0)=q_i$, and mapping i to j if $f_i(1)=q_j$. This recipe yields a homomorphism $T_\phi\colon\pi_1\to S_n$, and since X is connected, the image of T_ϕ is a transitive subgroup of S_n. By definition $T_\phi(\pi_1)=$ Mon (X,ϕ). Setting $G=T_\phi(\pi_1)$, $x_i=T_\phi(\gamma_i)$, $1\leqslant i\leqslant r$, we get that g, n, r are related by

$$\sum_{i=1}^{r}\operatorname{ind}x_i=2(n+g-1), \tag{4}$$

$$\langle x_1,\ldots,x_r\rangle=G,\qquad x_1\cdots x_r=1,\qquad x_i\neq 1,\ i=1,\ldots,r.$$

Furthermore, G is primitive if and only if $\mathbb{C}(\phi)$ is a maximal subfield of $\mathbb{C}(X)$. Riemann's existence theorem states that conversely, if G is a transitive subgroup of S_n and (4) holds, then for each r-element subset S of $\mathbb{P}^1$, there is (1) such that $S=\{x\in\mathbb{P}^1 \mid |\phi^{-1}(x)|<n\}$, and in addition, G and Mon (X,ϕ) are conjugate in S_n by an element which carries $T_\phi(\gamma_i)$ to x_i, $1\leqslant i\leqslant r$.

If G is a group and there is (1) such that X has genus g and Mon $(X,\phi)\cong G$, we say that G is a group of genus g.

In this paper, we restrict our attention to the case $g=0$. In this case, $\mathbb{C}(X)=\mathbb{C}(z)$ for some $z\in\mathbb{C}(X)$, and so ϕ is a rational function of z. Setting $z=\phi_0$, we invoke Luroth's theorem and factorize (1) via

$$X\xrightarrow{\phi_0}\mathbb{P}^1\xrightarrow{\phi_1}\mathbb{P}^1\longrightarrow\cdots\xrightarrow{\phi_h}\mathbb{P}^1$$

with $\phi=\phi_h\cdot\phi_{h-1}\cdot\cdots\cdot\phi_0$, in such a way that $\mathbb{C}(\phi_i)$ is a maximal subfield of $\mathbb{C}(\phi_{i-1})$, $i=1,\ldots,h$. By Proposition 2.1, the short proof of which we owe to Glauberman, we get

$$\operatorname{cf}(\operatorname{Mon}(X,\phi))\subseteq\bigcup_{i=1}^{h}\operatorname{cf}(\operatorname{Mon}(\mathbb{P}^1,\phi_i)). \tag{5}$$

Thus, in trying to show that $\mathscr{E}(0)$ is finite, we may restrict our attention to those groups G which satisfy the hypotheses of [AS] and in addition, have the property that (4) holds with $g = 0$, where ind is computed with respect to the action of G on the cosets of H. Such a group G is called a primitive group of genus 0. We are hoping to produce a finite set $\mathscr{E}$ of simple groups such that if G is any primitive group of genus 0, then every composition factor of G which is not in $\mathscr{E}$ is either a C_p or an A_n. By parsimony, we may take $\mathscr{E} = \mathscr{E}(0)$, although to a first approximation, we may settle for any set of simple groups which contains $\mathscr{E}(0)$ as a cofinite subset. Thus, for example, we could avoid any discussion of the sporadic groups, or we could adjoin to $\mathscr{E}(0)$ the set of all simple groups of order at most 10^{100}. Such a possibility has arisen in this paper, although hope still remains that $\mathscr{E}(0)$ may be explicitly determined. The following two results have already been obtained:

THEOREM C2 (Aschbacher [A]). *If G is a primitive group of genus* 0 *and* (C2) *in* [AS] *holds then $Q = L_1 \times L_2$, where $L_i \cong A_5$. Moreover, G/Q is abelian.*

THEOREM B (Shih [S]). *If G is a primitive group of genus* 0, *then* (B) *of* [AS] *does not hold.*

The object of this paper is to prove

THEOREM A. *If G is a primitive group of genus* 0 *and* (A) *of* [AS] *holds, then one of the following holds*:

(i) $G'' = 1$ *and* $n = p$ *or* p^2.

(ii) $p = 2$ *and* $n \leqslant 2^{16}$.

(iii) $p = 3$ *and* $n \leqslant 3^6$.

(iv) $p = 5$ *and* $n \leqslant 5^3$.

(v) $p = 7$ or 11 *and* $n = p^2$.

THEOREM C1. *If G is a primitive group of genus* 0, *then* (C1) *of* [AS] *does not hold.*

The next result shows that when $F^*(G)$ is not abelian, the structure of $G/F^*(G)$ is not arbitrary.

THEOREM D. *If G is a primitive group of genus* 0 *and $F^*(G)$ is non-abelian, then $\bar{G} = G/F^*(G)$ is solvable or $\bar{G}/S \cong A_5$ or S_5, where S is solvable.*

The next result deals with composition factors of $F^*(G)$.

THEOREM E. *Suppose G is a primitive group of genus 0 and L is a nonabelian simple subnormal subgroup of G. Then there exists a group M with $L \subseteq M \subseteq \mathrm{Aut}\, L$ and a subgroup K of M which does not contain L such that for some non identity element x of M,*

$$\frac{|x^M \cap K|}{|x^M|} > \frac{1}{85}.$$

Note that if $n \geqslant 5$ and $L = A_n$ we may take $M = L$, $K = A_{n-1}$, $x = (123)$. However, we conjecture that there is a number N such that if $q \geqslant N$ and L is a Chevalley group over $\mathbb{F}_q$, then M, K, x do not exist. We verify that this is the case for $L_2(p)$. This yields

COROLLARY F. *If p is a prime >341, then $L_2(p)$ is not a composition factor of any group of genus 0.*

There is no Theorem C3 in this paper, since the analysis of case (C3) of [AS] promises to be tough.

This paper is organized as follows. In Section 2, some general results are given. In Section 3, the case $F(G) \neq 1$ is first considered and we reduce to the case $O_p(G) = 1$ for $p > 85$. In Sections 4 through 8, the remaining cases are handled. In Section 9, Theorems E and F are proved.

As regards the proof of Theorem A for the case $G'' \neq 1$, in the course of the proof we find several but not all of the finitely many groups which satisfy (A) of [AS].

2. GENERAL RESULTS

PROPOSITION 2.1. *Let G be a finite group and let H, K be subgroups of G with $K \subseteq H \subseteq G$. Set*

$$V = \bigcap_{g \in G} H^g, \qquad U = \bigcap_{h \in H} K^h, \qquad W = \bigcap_{g \in G} K^g.$$

Then $\mathrm{cf}(G/W) \subseteq \mathrm{cf}(G/V) \cup \mathrm{cf}(H/U)$.

Proof. Without loss of generality, we assume that $W = 1$. Suppose $S \in \mathrm{cf}(G)$. Since $\mathrm{cf}(G) = \mathrm{cf}(G/V) \cup \mathrm{cf}(V)$, we may assume that $S \in \mathrm{cf}(V)$, and the proof will be complete if we can show that $S \in \mathrm{cf}(H/U)$. Choose M subnormal in V minimal with respect to $S \in \mathrm{cf}(M)$. The minimality of M guarantees that M has a unique maximal normal subgroup N and that $M/N \cong S$.

Now $V \lhd G$, $U \lhd H$, and so $\langle U^g, V \rangle \subseteq H^g$ for all g in G. Since

$$\bigcap_{g \in G} U^g = \bigcap_{g \in G} K^g = 1,$$

we get an embedding π of V into the direct product

$$\prod_{g \in G} H^g/U^g,$$

the map π sending v to the element whose g-component is $\pi_g(v) = vU^g$. Thus, we can choose g in G such that $\pi_g(M) \neq 1$, and for such a g, $M \cap \ker \pi_g \subseteq N$, as N contains all the proper normal subgroups of M. Since $V \lhd H^g$, so also $\pi_g(V) \lhd H^g/U^g$, and it follows that $\pi_g(M)$ is subnormal in H^g/U^g. Since $M \cap \ker \pi_g \subseteq N$, we get

$$M/N \cong \pi_g(M)/\pi_g(N) \in \mathrm{cf}(H^g/U^g).$$

Since $H^g/U^g \cong H/U$, and since $S \cong M/N$ we get $S \in \mathrm{cf}(H/U)$, as required.

COROLLARY 2.2. *If S is a composition factor of a group of genus zero, then S is a composition factor of a primitive group of genus zero.*

Proof. Suppose $S \in \mathrm{cf}(G)$, G being a group of genus zero. Let K be the stabilizer of a point, and let

$$K = K_0 \subset K_1 \subset \cdots \subset K_n = G$$

be a chain of subgroups each maximal in its successor. We view G as the monodromy group of a cover of $\mathbb{P}^1$ of degree $[G:K]$, the cover given by (1) of the Introduction. The chain connecting K to G induces a factorization of ϕ:

$$\phi: X = X_0 \xrightarrow{\phi_0} X_1 \xrightarrow{\phi_1} X_2 \longrightarrow \cdots \xrightarrow{\phi_{n-1}} X_n = \mathbb{P}^1.$$

The genus zero condition implies that $\mathbb{C}(X_0) = \mathbb{C}(t_0)$ for some $t_0 \in \mathbb{C}(X)$, and then Luroth's theorem gives $\mathbb{C}(X_i) = \mathbb{C}(t_i)$ for some t_i, $i = 0, 1, \ldots, n$. By construction, $\mathrm{Mon}(X_i, \phi_i)$ is a primitive group of genus zero. By the preceding proposition and an easy argument by induction on n, $S \in \mathrm{cf}(\mathrm{Mon}(X_i, \phi_i))$ for some i, and the proof is complete.

Throughout the remainder of this section, we assume that the group G acts faithfully and transitively on a set Ω, with $|\Omega| = n$. If $g \in G$, set $\mathrm{Fix}\, g = \{\omega \in \Omega \mid g\omega = \omega\}$, $f(g) = |\mathrm{Fix}\, g|$. We denote by $\mathrm{orb}\, g$ the number of orbits of $\langle g \rangle$ on Ω. Set $\mathrm{ind}\, g = n - \mathrm{orb}\, g$. The two results which we record here are well known and elementary, so no proofs are given.

LEMMA 2.3. (a) $\mathrm{ind}\, g \geqslant \mathrm{ind}\, g^k$ *for all* $g \in G$, $k \in \mathbb{Z}$.

(b) $\mathrm{orb}\, g = (1/d) \sum_{i=0}^{d-1} f(g^i)$, *where g has order d.*

PROPOSITION 2.4. *Suppose* $r \geq 2$, $G = \langle x_1, ..., x_r \rangle$, $\prod_{i=1}^{r} x_i = 1$, *and the order* d_i *of* x_i *is* > 1, $i = 1, ..., r$. *Then one of the following holds*:

(a) $\sum_{i=1}^{r} ((d_i - 1)/d_i) \geq 85/42$.

(b) $r = 4$, $d_i = 2$ *for each* i *and* $G'' = 1$.

(c) $r = 3$ *and (up to permutation)*, $(d_1, d_2, d_3) =$

(i) $(3, 3, 3)$, $(2, 3, 6)$, *or* $(2, 4, 4)$ *and* $G'' = 1$.

(ii) $(2, 2, d)$ *and* G *is dihedral.*

(iii) $(2, 3, 3)$ *and* $G \cong A_4$.

(iv) $(2, 3, 4)$ *and* $G \cong S_4$.

(v) $(2, 3, 5)$ *and* $G \cong A_5$.

(d) $r = 2$ *and* G *is cyclic.*

Remark. The proof of Proposition 2.4 is essentially simply a matter of inspection (cf. [M, II.4]).

The next observation is useful for keeping track of the various genus zero r-tuples for G. If $G = \langle x_1, ..., x_r \rangle$ with $x_1 \cdots x_r = 1$, then $G = \langle y_1, ..., y_r \rangle$ with $y_1 \cdots y_r = 1$, where $y_j = x_j$ if $j \notin \{i, i+1\}$, $y_i = x_{i+1}$, and $y_{i+1} = x_{i+1}^{-1} x_i x_{i+1}$. In particular, one can reorder the conjugacy classes occurring among the x_i's. See [A, Section 4] for more details.

3. THE CASE $F(G) \neq 1$: *The Generic Case*

Throughout this section, assume G acts primitively and faithfully on Ω, and we set

$$|\Omega| = n.$$

We also assume G has a minimal normal subgroup N which is Abelian, and we retain the notation of Section 2.

Choose $\omega \in \Omega$ and let $H = G_\omega$. Then by [H, Satz 3.2, p. 159], we have

$$G = HN, \qquad H \cap N = 1, \qquad N = C_G(N),$$

and

$$|N| = n = p^e,$$

for some prime p and natural number e. Furthermore, the map

$$\phi : N \to \Omega$$

$$x \to x\omega$$

is a bijection, and if $h \in H$, then $\phi(hxh^{-1}) = h\phi(x)$. Hence, in particular,

$$f(h) = |C_N(h)|, \qquad h \in H.$$

Viewing N as a vector space over $\mathbb{F}_p$, we see that if $g \in G$, conjugation by g induces a linear transformation of N, and we denote by $\det g$ the corresponding determinant.

LEMMA 3.1. *Suppose $x \in G$ and $x = yz = zy$, where y is a p-element and z is a p'-element. Then $f(x) \neq 0$ iff $f(y) \neq 0$.*

Proof. Since y is a power of x, we have

$$\text{Fix } x \subseteq \text{Fix } y, \qquad \text{so if } f(x) \neq 0, \text{ then } f(y) \neq 0.$$

Conversely, suppose $f(y) \neq 0$. Replacing x by a conjugate if necessary, we assume without loss of generality that $y \in H$. Set $G_0 = \langle N, x \rangle$, $X = \langle x \rangle$, $H_0 = G_0 \cap H$. Since N is a p-group, we have $X \cap N = \langle y \rangle \cap N$ and since $y \in H$, while $H \cap N = 1$, we get $X \cap N = 1$. Thus, X and H_0 are complements to N in G_0, and so are isomorphic, hence, both are cyclic; and both X and H_0 contain y. Thus $\langle z \rangle$ and the Hall p'-subgroup of H_0 are conjugate in $C_{G_0}(y)$, which means that X and H_0 are conjugate in G, whence $f(x) \neq 0$.

LEMMA 3.2. *Suppose $x \in G$ and $f(x) = 0$. Then*

$$\text{ind } x \geqslant \frac{p-1}{p} n.$$

Proof. Write $x = yz = zy$ as in the preceding lemma, and conclude that $f(y) = 0$. Since y is a power of x, we have $\text{ind } x \geqslant \text{ind } y$, so we assume without loss of generality that x is a p-element.

Since $f(x) = 0$ every orbit of $\langle x \rangle$ on Ω has cardinality a positive power of p, so $\text{orb } x \leqslant n/p$. The lemma follows.

LEMMA 3.3. *Suppose $x \in G$, x has order d and $f(x) \neq 0$. Then*

$$\text{ind } x \geqslant \left(\frac{d-1}{d}\right)\left(\frac{p^c - 1}{p^c}\right) n,$$

where

$$p^c = \min \{ |[x^j, N]| \mid j = 1, \ldots, d-1 \}.$$

Proof. Since $f(x) \neq 0$, we assume without loss of generality that $x \in H$. If $d = 1$, the lemma holds trivially. So we assume that $d > 1$. Since $x \in H$, we get for each j.

$$f(x^j) = |C_N(x^j)|.$$

Hence

$$\text{ind } x = n - \frac{1}{d}\sum_{j=0}^{d-1} f(x^j) \geqslant n - \frac{n}{d} - \frac{1}{d}\sum_{j=1}^{d-1}\frac{n}{p^c} = \left(\frac{d-1}{d}\right)\left(\frac{p^c-1}{p^c}\right)n.$$

LEMMA 3.4. *Suppose $x \in G$ has order d. Then*

$$\text{ind } x \geqslant \left(\frac{d-1}{d}\right)\left(\frac{p-1}{p}\right)n.$$

Proof. We assume without loss of generality that $x \neq 1$. If $f(x) = 0$, apply Lemma 3.2. If $f(x) \neq 0$, apply Lemma 3.3, observing that $c \geqslant 1$.

LEMMA 3.5. *Assume $G = \langle x_1, ..., x_s \rangle$.*

(a) *If x_i is a p'-element for each i, then*

$$\prod_{i=1}^{s} |[x_i, N]| > |N| \cdot |H^1(H, N)|.$$

(b) *If $f(x_i) > 0$ for each i, then $\prod_{i=1}^{s} |[x_i, N]| > |N|$.*

Proof. We prove only (b). The proof of (a) is similar, and we shall only use the statement of (b).

Write $x_i = h_i v_i$ with $h_i \in H$, $v_i \in N$. Since $f(x_i) > 0$, x_i is conjugate to h_i, and so $v_i \in [h_i, N]$ for each i. Since $G = \langle x_1, ..., x_s \rangle$, so also $H = \langle h_1, ..., h_s \rangle$. If $v \in N$, then $H^v = \langle h_1 w_1, ..., h_s w_s \rangle$ with $w_i \in [h_i, N]$. Moreover, $H^v \neq H^w$ if v, w are distinct elements of N. Thus the map $\phi: N \to N \times \cdots \times N$ (s-fold product of N) defined by $\phi(v) = (w_1, ..., w_s)$ is injective and its image is contained in $W = [h_1, N] \times \cdots \times [h_s, N]$. Moreover, $\phi(N) \neq W$, since $(v_1, ..., v_s)$ is not in $\phi(N)$. Thus $|W| > |N|$, as desired.

The proof of (a) differs only in that ϕ is defined for every complement of N not just those conjugate to H.

PROPOSITION 3.6. *Assume $H = \langle h_1, h_2 \rangle$ with $h_1 h_2 h_3 = 1$. The following are equivalent:*

(a) *$\exists v_i \in N \ni x_i = h_i v_i$ is conjugate to h_i with $x_1 x_2 x_3 = 1$ and $G = \langle x_1, x_2 \rangle$.*

(b) *$|C_E(h_3)| < |[h_1, N] \cap [h_2, N]|$, where E is the subgroup of* Der(H, N) *consisting of the elements inner on $\langle h_1 \rangle$ and $\langle h_2 \rangle$.*

Proof. Assume (a) holds. By conjugating by an element of N, we can assume $x_3 = h_3$. Set $W = \{(w_1, w_2) \in N \times N \mid w_i \in [h_i, N]$ and $w_1 h_2 w_2 = h_2\}$. Clearly, $|W| = |[h_1, N] \cap [h_2, N]|$.

In order to show that (a) implies (b), we recall that

$$\mathrm{Der}(H, N) = \{\delta : H \to N \mid \delta(hh') = \delta(h)^{h'} \delta(h')\}.$$

Now if δ is an element of $\mathrm{Der}(H, N)$ and we set $H^\delta = \{h\delta(h) \mid h \in H\}$, then H^δ is a complement to N in G, and so the map which associates to δ the subgroup H^δ is a bijection between $\mathrm{Der}(H, N)$ and the set of all complements of N. If $\delta \in C_E(h_3)$, then H^δ is a complement to N with $(\delta(h_1), \delta(h_2)) \in W$. Hence $|C_E(h_3)| \leqslant |W|$. Since (a) holds, the pair (v_1, v_2) is in W, but is not of the shape $(\delta(h_1), \delta(h_2))$ for any δ in $C_E(h_3)$, and so (b) holds.

Conversely, if $|C_E(h_3)| < |W|$, we can choose (v_1, v_2) in W which is not of the shape $(\delta(h_1), \delta(h_2))$ for any δ in $C_E(h_3)$. Hence $\langle h_1 v_1, h_2 v_2 \rangle$ does not generate a complement, and by maximality of H, we get $G = \langle h_1 v_1, h_2 v_2 \rangle$ with $h_1 v_1 h_2 v_2 h_3 = 1$.

A special case worth noting is when $G = \langle x_1, x_2, x_3 \rangle$, $x_1 x_2 x_3 = 1$, x_1 is a reflection on N and $f(x_i) > 0$ for each i. The preceding proposition then implies that $[x_2, N] = [x_3, N] = N$. See [N] for generalizations.

We can easily handle the case of large p.

PROPOSITION 3.7. *If* $G = \langle x_1, ..., x_r \rangle$, $x_1 \cdots x_r = 1$ *and* $\sum_{i=1}^r \mathrm{ind}\, x_1 = 2n - 2$, *then either* $p < 85$ *or* $G'' = 1$.

Proof. We assume without loss of generality that for each $i = 1, ..., r$, the order of x_i is $d_i > 1$. By Lemma 3.4, $\mathrm{ind}\, x_i \geqslant (1 - d_i^{-1})(1 - p^{-1})\, n$. Thus,

$$2n > 2n - 2 = \sum_{i=1}^{r} \mathrm{ind}\, x_i \geqslant n(1 - p^{-1}) \sum_{i=1}^{r} (1 - d_i^{-1}).$$

Suppose $p > 85$. The preceding inequalities then imply that

$$\sum_{i=1}^{r} (1 - d_i^{-1}) < \frac{85}{42}.$$

Hence, Proposition 2.4(a) does not hold. Since $p > 85$, Proposition 2.4(c) (iv) does not hold, nor does (c)(v). Examination of the remaining possibilities in Proposition 2.4 shows that $G'' = 1$.

If $G'' = 1$, then as H acts irreducibly and faithfully on N, H is cyclic. Zariski [Z, pp. 21–23] found all examples of such groups of genus zero.

PROPOSITION 3.8 (Zariski). *If* $G = \langle x_1, ..., x_r \rangle$, $x_1 \cdots x_r = 1$ *with* x_i *of order* $d_i > 1$, $\Sigma\, \mathrm{ind}\, x_i = 2n - 2$, *and* $G'' = 1$, *then* $H \cong G/N$ *has order* 1, 2, 3, 4, *or* 6 (*with* $p \nmid |H|$) *and* $n = p$ *if* $p \equiv 1 \pmod{|H|}$. *If* $p \not\equiv 1 \pmod{|H|}$, *then* $n = p^2$. *Moreover, either* $r = 4$ *and* $d_i = 2$ *for each* i *or* $r \leqslant 3$.

Proof. If $G = N$, then $H = 1$, $|G| = p$, and we observe that $r = 2$.

If $G \neq N$, then as $N = C_G(N)$, we get that $N = G'$ and G is a Frobenius group with cyclic complement. In particular, G is not cyclic and so $r \geqslant 3$. If $x \in G$ has order d, then either $d = p$ and $\operatorname{ind} x = ((d-1)/d)n$ or $(p, d) = 1$ and $\operatorname{ind} x = (1 - d^{-1})(n-1)$. Thus,

$$2n - 2 = \sum_{i=1}^{r} \operatorname{ind} x_i \geqslant (n-1) \sum_{i=1} (1 - d_i^{-1}).$$

Thus $\sum_{i=1}^{r} (1 - d_i^{-1}) \leqslant 2$. Hence, one of the following holds:

(a) $r = 4$, $d_i = 2$ for each i.

(b) $r = 3$ and (up to permutation) $(d_1, d_2, d_3) =$

(i) $(2, 4, 4)$

(ii) $(2, 3, 6)$

(iii) $(3, 3, 3)$

(iv) $(2, 2, d)$

(v) $(2, 3, 3)$

(vi) $(2, 3, 4)$

(vii) $(2, 3, 5)$

Since $G'' = 1$, cases (b) (vi), (b)(vii) are excluded. Since N is an irreducible module for H, easy arguments complete the proof.

The main result of this paper follows along the lines of the proofs of the preceding results. The main tools are Proposition 2.4 and Lemmas 3.3, 3.4, and 3.5. As p becomes smaller, there are more cases to consider. The arguments are all relatively straightforward except for $p = 2$, where we invoke several times the results of McLaughlin on irreducible groups generated by transvections.

For future use, we record some additional results.

LEMMA 3.9. *Let $x = hn$, $h \in H$, $n \in N$. Then* $\operatorname{ind} x \geqslant \operatorname{ind} h$ *with equality if and only if x is conjugate to h.*

Proof. If x is not conjugate to h, then x is not conjugate to any element of H, and $f(x) = 0 < f(h)$. The same argument applies to each element of $\langle x \rangle$. Now apply Lemma 2.3(b).

LEMMA 3.10. *Let $x \in G$ be of order d with $d > 1$. Assume $p \nmid d$.*

(a) *If d is a prime power, then*

$$\operatorname{ind} x \geqslant (1 - p^{-b})(1 - d^{-1})\, n,$$

where b is the smallest positive integer such that $p^b \equiv 1 \pmod{d}$.

(b) *If* $\det x = 1$, *then*

$$\operatorname{ind} x \geqslant (1-p^{-2})(1-d^{-1}).$$

Proof. (a) We may assume that $x \in H$. Write $N = N_1 \times \cdots \times N_t$, where $\langle x \rangle$ acts irreducibly on each N_i. Since d is a prime power, we may assume notation is chosen so that $\langle x \rangle$ acts faithfully on N_1. Then $|N_1| = p^b$, where b is as given. Thus $N_1 \subseteq [x^j, N]$ for $j = 1, \ldots, d-1$. Now apply Lemma 3.3.

(b) If $1 \leqslant j \leqslant d-1$, then $\det x^j = 1$; and since then $p \nmid d$, we get $|[x^j, N]| > p$, whence

$$p^c = \min\{|[x^j, N]| \mid j = 1, 2, \ldots, d-1\} \geqslant p^2.$$

LEMMA 3.11. *Let* $x \in G$ *of order* $d > 2$.

(a) *If* $p > 11$, *then* $\operatorname{ind} x \geqslant \frac{8}{13} \cdot n$.

(b) *If* $p = 11$, *then* $\operatorname{ind} x \geqslant \frac{80}{121} \cdot n$.

(c) *If* $p = 5$, $\operatorname{ind} x \geqslant \frac{3}{5} n$.

(d) *If* $p = 3$, $\operatorname{ind} x \geqslant \frac{4}{9} n$.

Proof. (a) and (d) follow by Lemma 3.3. In cases (b) and (c), Lemma 3.3 applies if $d > 3$. For $d = 3$, use Lemma 3.7.

Remark. The previous lemma explicitly avoids the prime 7.

4. The Case of Many Branch Points

We keep the same assumptions and notation of the previous section and we also assume that $G'' \neq 1$. Fix a system of generators $x_1, \ldots, x_r$ of G with $\prod_{i=1}^r x_i = 1$, $\sum_{i=1}^r \operatorname{ind} x_i = 2n-2$, and such that x_i has order $d_i > 1$, $i = 1, 2, \ldots, r$. We wish to find all possibilities with $r \geqslant 4$. Unfortunately, the problem is not settled for $p = 2$ or 3.

If X is a subgroup of G, denote by X^+ the set of elements of X which induce by conjugation an automorphism of N of determinant 1.

First, note that by Lemma 3.4, if x is a non-identity element of G, then $\operatorname{ind} x \geqslant \frac{1}{4} n$ (see also [FG]). Thus

$$r \leqslant 7. \tag{4.1}$$

Indeed, as $\operatorname{ind} x \geqslant ((p-1)/2p)\, n$, the same argument shows that

$$\begin{aligned} &\text{(a)} \quad \text{If} \quad p = 3, \quad r \leqslant 5. \\ &\text{(b)} \quad \text{If} \quad p > 3, \quad r \leqslant 4. \end{aligned} \tag{4.2}$$

We first treat the case $p>3$, $r=4$. Since $G''\neq 1$, Proposition 2.4 implies that some d_i exceeds 2, say d_4. By Lemma 3.4 and Lemma 2.3(a), it follows that for $p>11$

$$\sum_{i=1}^{4} \operatorname{ind} x_i \geqslant (\tfrac{3}{2}+\tfrac{2}{3})(\tfrac{12}{13})\, n = 2n.$$

So $p\leqslant 11$. If $p=11$, then by Lemma 3.11(b), $\operatorname{ind} x_4 \geqslant \frac{80}{121}n$, and so by Lemma 3.4

$$\sum_{i=1}^{4} \operatorname{ind} x_i \geqslant (\tfrac{3}{2}\cdot\tfrac{10}{11}+\tfrac{80}{121})\, n > 2n.$$

Next consider $p=7$. If $d_i>2$ for some $i\leqslant 3$, then Lemma 3.4 yields

$$\sum_{i=1}^{4} \operatorname{ind} x_i \geqslant (1+\tfrac{4}{3})\cdot\tfrac{6}{7}n = 2n.$$

So $d_1=d_2=d_3=2$. Since $\operatorname{ind} x_4 < 2n-\frac{9}{7}n=\frac{5}{7}n$, Lemma 3.4 implies that $d_4<6$. Lemmas 3.2 and 3.3 then imply that $d_4=3$. Since the product of the x_i's is 1, this implies that $\det x_4=1$, and so $|[x_4, N]|\geqslant 49$, whence $\operatorname{ind} x_4 \geqslant \frac{32}{49}n$. Also, $\det x_i=1$ for some $i\leqslant 3$, and so $\operatorname{ind} x_3 \geqslant \frac{24}{49}n$. Thus,

$$\sum_{i=1}^{4} \operatorname{ind} x_i \geqslant (2\cdot\tfrac{3}{7}+\tfrac{24}{49}+\tfrac{32}{49})\cdot n = 2n.$$

Finally, consider the case $p=5$. If x has order >2, then $\operatorname{ind} x \geqslant \frac{3}{5}n$, while if x has order 2, $\operatorname{ind} x \geqslant \frac{2}{5}n$. Thus, $d_1=d_2=d_3=2$. Also, if $|[x_i, N]|>5$ for each $i<4$, then $\operatorname{ind} x_i \geqslant \frac{12}{25}n$, and

$$\sum_{i=1}^{4} \operatorname{ind} x_i \geqslant \tfrac{36}{25}n+\tfrac{3}{5}n > 2n.$$

So we can assume without loss of generality that x_1 acts as a reflection on N. If x_1, x_2, x_3 are all reflections, then Lemma 3.5 implies $e=2$. Then $\det x_4=-1$ and so d_4 is even while $\operatorname{ind} x_4=18$. This implies $d_4=4$ and x_4 N is central in G/N. Since H is not abelian, it follows that $G/\langle N, x_4\rangle$ is not cyclic. Replacing our 4-tuple by a conjugate, we assume without loss of generality that $x_4\in H$. Then $H/\langle x_4\rangle$ is generated by three involutions whose product is 1. So $\langle x_4\rangle = Z(H)$, $H/Z(H)$ is a four-group and $|H|=16$.

If x_2 is a reflection while x_3 is not, then Lemma 3.5 implies $|[x_3\ N]|\geqslant 5^{e-1}$. If $e\geqslant 4$, this implies that $[x_3, N]\cap C_N(x_1)\cap C_N(x_2)$ is a nontrivial normal subgroup of G, a contradiction.

If $e=3$, then the same argument applies unless $|[x_3, N]|=25$. Then ind $x_4=88$, det $x_4=1$. This fails by inspection. If $e=2$, Nx_3 is central in G/N, det $x_4=1$, ind $x_4=16$. Then $d_4=3$ or 5 and $f(x_4)>0$. If $d_4=5$, then H contains a transvection, whence $H'\cong SL_2(5)$. This is false, as $H/Z(H)$ is generated by two involutions and so H is solvable. If $d_4=3$, then $H/Z(H)\cong S_3$ while $H\cong D_6$, the dihedal group of order 12.

If neither x_2 nor x_3 is a reflection, then ind $x_j\geqslant\frac{12}{25}n$ for $j=2, 3$. Since det $x_4=\pm 1$ ind $x_4\geqslant\frac{16}{25}n$, whence $\sum_{i=1}^{4}$ ind $x_i\geqslant 2n$. So we have proved.

THEOREM 4.1. *If $p>3$ and $r>3$, then either $G''=1$ or $p=5$, $e=2$, $r=4$, and (up to permutation) $d_1=d_2=d_3=2$ and $d_4=3$ or 4. If $d_4=3$, then $H\cong D_6$, and if $d_4=4$, then H is isomorphic to a Sylow 2-subgroup of the subgroup of index 2 in $GL_2(5)$.*

Now consider $p=3$. Assume that $r=5$. Write $x_i=h_iu_i$ with $h_i\in H$, $u_i\in N$. Thus,

$$H=\langle h_1, \ldots, h_5\rangle, \qquad h_1\cdot h_2\cdot h_3\cdot h_4\cdot h_5=1.$$

Using Lemma 3.4, we see that either $d_i=2$ and $|[x_i, N]|=3$, or ind $x_i\geqslant\frac{4}{9}n$. Thus at least three of the x_i are reflections. We assume without loss of generality that x_1, x_2, and x_3 are reflections. Since the product of x_i's is 1, one of x_4 or x_5 is not a reflection, and so we assume without loss of generality that x_5 is not a reflection.

Case 1. x_4 is a reflection. By Lemma 3.5, we have $e\leqslant 3$. Moreover, det $x_5=1$ and ind $x_5=\frac{2}{3}n-2$. By Lemma 3.4, we get $d_5=2$, 3, or 6.

Case 1a. $d_5=2$. Here we have ind $x_5=\frac{1}{2}(n-3^l)=\frac{2}{3}n-2$, where $|C_N(x_5)|=3^l$. This forces $l=0$, $e=2$. Set $h_4'=h_4h_5$. Since h_5 inverts N, h_4' is an involution and, in addition, $h_1h_2=h_4'h_3=h$, say, with $\langle h\rangle\lhd H$. Also, h is inverted by h_1, h_2, h_3, h_4. Since H acts irreducibly on N, it follows that $H\cong D_4$.

Case 1b. $d_5=3$. If $f(x_5)=0$, then ind $x_5=\frac{2}{3}n$. If $f(x_5)\neq 0$, then ind $x_5=\frac{2}{3}(n-3^l)$. where $|C_N(x_5)|=3^l$. Since ind $x_5=\frac{2}{3}n-2$, we get $l=1$ and $f(x_5)\neq 0$. Thus $e\leqslant 3$. If $e=2$, then $H\cong GL_2(3)$, since G/N contains a transvection and $|G:G^+|=2$. Suppose $e=3$. Then Σ dim$[x_i, N]=5<2e$, and a variation of Proposition 3.6 (see [N]) shows this is impossible.

Case 1c. $d_5=6$. If $e=2$, then as det $x_5=1$, we get ind $x_5=6$ and ind $x_i=3$ for $i<5$. Thus, $\sum_{i=1}^{5}$ ind $x_i=18$, which is not $2(n-1)$, so this case is excluded. If $e=3$, then ind $x_i=9$ for $i<5$, whence ind $x_5=16$. Since det $x_5=1$, $f(x_5^3)=3$. Thus $f(x_5)\leqslant 3$ and so ind $x_5\geqslant 18$, a contradiction which shows that this case is also excluded.

Case 2. x_4 is not a reflection. Here we get ind $x_i \geq \frac{4}{9}n$ for $i \geq 4$. Hence, for $j \geq 4$, we get ind $x_j < \frac{5}{9}n$ and so $d_j < 4$. By considering determinants, we can assume without loss of generality that $d_4 = 2$, and det $x_4 = -1$. Since x_4 is not a reflection, it follows that $e \geq 3$ and ind $x_4 \geq \frac{13}{27}n$.

First, suppose $e > 3$. If x_4 inverts N, then $1 \neq C_N(x_1) \cap C_N(x_2) \cap C_N(x_3) = D$, and D is G-invariant. This is not the case, and so we conclude that $C_N(x_4) \neq 1$. Thus, ind $x_i \equiv 0 \pmod 3$ for $1 \leq i \leq 4$. Since $2(n-1) \not\equiv 0 \pmod 3$, we conclude that ind $x_5 \not\equiv 0 \pmod 3$. This in turn forces $d_5 = 3$, $f(x_5) = 3$, whence

$$\text{ind } x_5 = n - \left(3 + \frac{n-3}{3}\right) = \frac{2}{3}n - 2,$$

and as ind $x_i = \frac{1}{3}n$ for $1 \leq i \leq 3$, we get

$$\text{ind } x_4 = \tfrac{1}{3}n.$$

This means that x_4 is a reflection, which is false.

Now suppose that $e = 3$. In this case, x_4 inverts N, and so det $x_5 = 1$, ind $x_5 = 12$. This leaves the possibilities:

(a) $d_5 = 2$ and $|[x_5, N]| = 9$,

(b) $d_5 = 3$ and $|[x_5, N]| = 3$ and $f(x_5) > 0$.

In case (*a*), $H/Z(H)$ is generated by three elements, each of order 1 or 2, whose product is of order 1 or 2. Thus H is solvable. It follows easily that $F(H) = O_2(H)$ is Abelian of rank at least 2. Thus $H \subseteq M$, where M is the monomial subgroup of $GL_3(3)$. Since $Z(H) \neq 1$ and since H acts irreducibly on N and is generated by involutions, we get $H = M$. However $H/Z(H) \cong S_4$ and S_4 can not be generated by four element of orders 1 or 2 whose product is 1. So (a) cannot hold.

Suppose (b) holds. Consider the action of G on X, the set of 13 lines in N. Let $\sigma(x_i)$ be the index of x_i as a permutation on X. Then $\sigma(x_1) = \sigma(x_2) = \sigma(x_3) = 4$, $\sigma(x_4) = 0$, and $\sigma(x_5) = 6$. Thus $\Sigma\, \sigma(x_i) = 18 < 24$. Hence G does not act transitively on X. However, as H acts irreducibly on N and contains a transvection, $H \geq SL_3(3)$. Thus G does act transitively on X, a contradiction, Putting these pieces together, we get:

THEOREM 4.2. *If* $p = 3$ and $r > 4$, *then* $r = 5$ *and one of the following holds*:

(a) $n = 9$, $d_i = 2$ *for each* i, *and* $H \cong D_4$.

(b) $n = 9$, $d_i = 2$, *if* $1 \leq i \leq 4$, $d_5 = 3$ (*up to reordering*) *and* $H \cong GL_2(3)$.

We postpone our discussion of the cases $p=2$ to Section 8 and $p=3$, $r=4$ to Section 7.

5. The Case $p>5$

In this section, we assume $G=\langle x_1, x_2, x_3\rangle$, $x_1x_2x_3=1$, x_i of order $d_i>1$, and $N=F(G)=O_p(G)$, $p>5$. Moreover, we assume that G acts primitively and faithfully on a set Ω with $|\Omega|=n=p^e$ and $G''\neq 1$. Set $\bar{G}=G/N$. We shall prove the following result:

Theorem 5.1. *If Σ ind $x_i=2n-2$, then (up to permutation) one of the following holds*:

(a) $p=7$, $e=2$, $(d_1, d_2, d_3)=(2, 4, 6)$ and $\bar{G}\cong C_3\cdot D_4$.

(b) $p=11$, $e=2$, $(d_1, d_2, d_3)=(2, 3, 8)$ and $\bar{G}\cong GL_2(3)$.

We prove Theorem 5.1 by a sequence of results. We assume without loss of generality that $d_1\leqslant d_2\leqslant d_3$.

(5.2) *If $d_1>2$,* then Theorem 5.1 holds.

Proof. By Proposition 2.4, $d_3>3$. Hence Lemma 3.4,

$$\Sigma \text{ ind } x_i\geqslant\left(\frac{2}{3}+\frac{2}{3}+\frac{3}{4}\right)\left(\frac{p-1}{p}\right)n=\frac{25}{12}\left(\frac{p-1}{p}\right)n.$$

Thus $p\leqslant 23$. If $p=11$ or 23, ind $x_i\geqslant\frac{80}{121}n$ for $i=1, 2$ (see Lemma 3.11) and ind $x3\geqslant\frac{8}{11}n$ (see Lemmas 3.2 and 3.3). Thus Σ ind $x_i>2n$. If $p=17$, ind $x_i\geqslant\frac{192}{289}n$ and ind $x_3\geqslant\frac{12}{17}n$. Thus Σ ind $x_i>2n$. Suppose $p=13$. Then ind $x_i\geqslant\frac{112}{169}$ unless x_i is a reflection of order 3 (and so ind $x_i=\frac{8}{13}n$). So we can assume $d_1=3$ and ind $x_1=\frac{8}{13}n$ (or Σ ind $x_i>2n$). It follows by Lemma 3.5 that neither x_2 nor x_3 is a reflection. Hence ind $x_2\geqslant\frac{112}{169}n$, ind $x_3\geqslant\frac{126}{169}$, and Σ ind $x_i>2n$. Next suppose $p=19$. Then ind $x_i\geqslant\frac{240}{361}n$ unless x_i is a reflection of order 3 with ind $x_i=\frac{12}{19}n$. Since $d_3>3$, ind $x_3\geqslant\frac{270}{361}n$. Thus x_1 and x_2 must be reflections. This contradicts Lemma 3.5.

Now consider $p=7$. If $d_i>3$, then using Lemmas 3.2, 3.3, 3.4, it is easy to see that ind $x_i\geqslant\frac{5}{7}n$. Hence if $d_2>3$,

$$\Sigma \text{ ind } x_i\geqslant(\tfrac{4}{7}+2\tfrac{5}{7})n=2n.$$

Thus $d_1=d_2=3$. If neither x_1 nor x_2 acts as a reflection on N, then ind $x_i\geqslant\frac{32}{49}n$ and Σ ind $x_i>2n$. So assume x_1 is a reflection. By Lemma 3.5, $[x_2, N]=N$. Since $G=\langle x_1, x_2\rangle$ acts absolutely irreducibly on N (as x_1 is

a reflection), x_1 and x_2 have no common eigenspace on N. Thus $e=2$. Since x_2 is not a scalar, $\det x_2=1$. Thus $\det x_1$ and $\det x_3$ have order 3. Thus d_3 is a multiple of 3. Since $\operatorname{ind} x_1=28$ and $\operatorname{ind} x_2=32$, it follows that $\operatorname{ind} x_3=36$. This implies $d_3\leqslant 7$ by Lemma 3.4. Hence $d_3=6$. However, $\det x_3$ is of order 3 and is not a scalar transformation on N. So x_3 has eigenvalues -1 and λ, where λ has order 6; whence $\operatorname{ind} x_3=38\neq 36$.

(5.3) If $(d_1, d_2)=(2, 3)$, Theorem 5.1 holds.

Proof. By Proposition 2.4, $d_3>6$. If x_2 is a reflection, then Lemma 3.5 implies $[x_1, N]=N$. Then x_1 acts as a scalar on N contradicting the irreducibility of G on N.

If x_1 is a reflection, then Lemma 3.5 implies $[x_2, N]=N$. Since no eigenspace of x_2 over the algebraic closure of F_p can be more than one-dimensional, $e=2$, and $\det x_2=1$. Thus $\operatorname{ind} x_1=\frac{1}{2}(n-p)$ and $\operatorname{ind} x_2=\frac{2}{3}(n-1)$. Hence $\operatorname{ind} x_3=\frac{5}{6}p^2+\frac{1}{2}p-\frac{4}{3}$ and $\det x_3=-1$. In particular, d_3 is even. If $f(x_3)=0$, then $[x_3, N]\neq N$. Since $\det x_3=-1$, this implies $d_3=2p$, and so $\operatorname{ind} x_3=p^2-\frac{1}{2}(p+1)$. This contradicts the above equality (since $p\neq 5$). So assume $f(x_3)>0$. If $p\mid d_3$, then as $\det x_3=-1$, $d_3=4p$, and $\operatorname{ind} x_3=p^2-\frac{1}{2}(p+1)$, a contradiction as before. If $(p, d_3)=1$, then as $\det x_3=-1$, either $d_3\equiv 2 \bmod 4$ and the eigenvalues of x_3 have order d_3 and $d_3/2$ or $d_3\equiv 0 \bmod 4$. In the first case $d_3\mid(p-1)$. Hence $d_3\geqslant 10$, $p\geqslant 11$, and so

$$\operatorname{ind} x_3=\frac{d_3-1}{d_3}(p^2-p)+\frac{d_3-2}{d_3}(p-1)>\frac{5}{6}p^2+\frac{1}{2}p-\frac{4}{3}.$$

In the second case, $\operatorname{ind} x_3=((d_3-1)/d_3)(p^2-1)$ which contradicts the earlier equality unless $p=11$ and $d_3=8$. Since $GL_2(3)$ is a $(2, 3, 8)$ group and does embed in $GL_2(11)$, there exist $h_i\in GL_2(3)\leqslant GL_2(11)$ with $h_1h_2h_3=1$ and h_i of order d_i. Since $[h_2, N]=N$, one can choose $1\neq v\in[h_1, N]$ so that $G=\langle h_1v, v^{-1}h_2, h_3\rangle$. By a counting argument, any $y_1, y_2, y_3\in GL_2(11)$ with y_i of order d_i and $y_1y_2y_3=1$ must generate a $GL_2(3)$. This is case (b) of Theorem 5.1.

So now assume that neither x_1 nor x_2 is a reflection. Thus $e\geqslant 3$. Then $\operatorname{ind} x_1\geqslant\frac{1}{2}((p^2-1)/p^2)\,n$ and $\operatorname{ind} x_2\geqslant\frac{2}{3}((p^2-1)/p^2)\,n$. Thus

$$\operatorname{ind} x_3<\left(2-\frac{7}{6}\left(\frac{p^2-1}{p^2}\right)\right)n.$$

First consider $p=7$. Thus $\operatorname{ind} x_3<\frac{6}{7}n$. Hence $f(x_3)>0$. Also, it follows that $d_3=7$ or 14. (If $7\nmid d$, use Lemma 3.9 to conclude that $\operatorname{ind} x\geqslant\frac{6}{7}n$ for any x of prime power order $d>7$. Then, using Lemma 3.3, it suffices to check the inequality holds for $d=10$, 12, and 15. Similarly, we check the

inequality for $d = 21$, 28, 35, and 49.) If $d_3 = 7$, then since Σ ind $x_i \equiv -2$ mod 7, ind $x_1 \equiv 0$ mod 7 (as $[x_1, N] \neq N$), and ind $x_3 \equiv 0$ or 1 mod 7, it follows that ind $x_2 \equiv 4$ mod 7 and ind $x_3 \equiv 1$ mod 7. Then ind $x_2 = \frac{2}{3}(n-1)$ and ind $x_3 = \frac{6}{7}(n-7)$. Hence ind $x_1 = \frac{10}{21}n + \frac{14}{3} < \frac{24}{49}n$ for $e > 3$. This contradicts the fact that x_1 is not a reflection. So $e = 3$. Since G is a (2, 3, 7)-group, G is perfect. Now det $x_2 = 1$ and $[x_2, N] = N$ imply x_2 acts as a scalar, a contradiction. If $d_3 = 14$, then as ind $x_3 < \frac{6}{7}n$ and ind $x_3 \not\equiv 0$ mod 7 (as in the previous case), it follows that $e = 3$ (use Lemma 3.3). Moreover, det $x_3 = -1$. Thus det $x_1 = -1$. This contradicts the fact that x_1 is neither a reflection nor a scalar on N.

Now assume $p > 7$. If $d_3 = 7$, then as a (2, 3, 7)-group is perfect, det $x_i = 1$ for each i. Thus ind $x_3 \geqslant \frac{6}{7}((p^2-1)/p^2)\,n$ and Σ ind $x_i > 2n$. So $d_3 > 7$. Since ind $x_3 \geqslant [(d_3-1)/d_3][(p-1)/p]\,n$, and ind $x_3 < \frac{5}{6}((p^2-1)/p^2)\,n$, it follows that

$$\frac{d_3-1}{d_3} < \frac{5}{6}\frac{p+1}{p} \leqslant \frac{5}{6}\frac{12}{11} = \frac{10}{11}.$$

Hence $d_3 < 11$. If $d_3 = 8$ or 9, then since det x_3 cannot have order d_3, ind $x_3 \geqslant \frac{7}{8}((p^2-1)/p^2)\,n$, a contradiction. So $d_3 = 10$, $p = 11$. Since ind $x_3 < \frac{100}{121}n$, it follows that x_3 is a reflection, but then det $x_1 x_2 x_3 \neq 1$.

(5.4) If $(d_1, d_2) = (2, 4)$, then Theorem 5.1 holds.

Proof. If x_2 is a reflection, then by Lemma 3.5, $[x_1, N] = N$ whence $\langle x_1, x_2 \rangle$ does not act irreducibly on N. If x_1 is a reflection, then $[x_2, N] = N$. Since G acts absolutely irreducibly on N, no eigenvalue of x_2 over the algebraic closure of F_p can occur with multiplicity more than one. Hence $e \leqslant 3$. If $e = 3$, ind $x_1 = \frac{1}{2}(p^3 - p^2)$ and ind $x_2 = \frac{1}{2}(p-1) + \frac{3}{4}(p^3 - p)$. Moreover, det $x_1 = \det x_2 = -1$. Thus det $x_3 = 1$ and

$$\text{ind } x_3 = \frac{3}{4}p^3 + \frac{1}{2}p^2 + \frac{1}{4}p - \frac{3}{2} \geqslant \frac{d_3-1}{d_3}(p^3 - p^2).$$

In particular, if $p \nmid d_3$, then ind $x_3 \geqslant [(d_3-1)/d_3](p^3 - p)$. This implies that (d_3, p) must be one of the following:

(i) $(5, p)$, $p < 13$, or

(ii) $(d_3, 7)$ with $d_3 = 6$, 7, or 14.

If $d_3 = 5$, then as ind $x_3 \equiv -\frac{3}{2}$ mod p, $[x_3, N] = N$, and ind $x_3 = \frac{4}{5}(p^3 - 1) \equiv -\frac{4}{5}$ mod p. Thus $p = 7$. However, no element of order 5 acts on a three-dimensional space over the field F_7. So we assume $p = 7$ and $d_3 = 6$, 7, or 14. The congruence ind $x_3 \equiv -\frac{3}{2}$ mod p eliminates $d_3 = 7$. If $d_3 = 6$, then $[x_3, N] = N$ (since x_1 is a reflection). Since det $x_3 = 1$ and

$\langle x_1, x_3\rangle$ acts irreducibly, x_3 must have one eigenvalue each of order 2, 3, and 6. (Then ind $x_3 = 282$ and Σ ind $x_i = 2n-2$.) If we fix the eigenvalues of x_3 (note there are two possibilities), then a straightforward matrix argument shows that $\langle x_1, x_2\rangle$ acts reducibly. If $d_3 = 14$, inspection of the various possibilities shows that ind $x_3 \geqslant 291$ and Σ ind $x_i > 2n-2$.

Next consider the case $e=2$. Then ind $x_1 = \frac{1}{2}(p^2-p)$ and det $x_1 = -1$. Since $[x_2, N] = N$ and x_2 is not a scalar, det $x_2 = 1$ or has order 4. In particular, det x_3 has order 2 or 4 (and so d_3 is even). If det x_2 has order 4, then $p \equiv 1 \bmod 4$ and $d_3 \equiv 0 \bmod 4$. By Lemma 3.4,

$$\sum_{i=1}^{3} \text{ind } x_i \geqslant \left(\frac{1}{2}+\frac{3}{4}+\frac{7}{8}\right)\left(\frac{p-1}{p}\right) n \geqslant 2n$$

unless $p < 17$. So $p = 13$. Then ind $x_3 = 135$. However, det x_3 has order 4 with $d_3 \geqslant 8$ implies ind $x_3 \geqslant 147$. If det $x_2 = 1$, then ind $x_2 = \frac{3}{4}(p^2-1)$ and so

$$\text{ind } x_3 = \frac{3}{4}p^2 + \frac{1}{2}p - \frac{5}{4} \geqslant \frac{d_3-1}{d_3}(p-1)\,p.$$

If $d_3 = 6$, then as det $x_3 = -1$, $p \equiv 1 \mod 3$ and ind $x_3 = \frac{2}{3}(p-1) + \frac{5}{6}(p^2-p)$. This implies $p = 7$. Inspection then shows $G/N \cong C_3 \cdot D_4$. This is case (a) of Theorem 5.1. If $d_3 \geqslant 8$, the inequality above implies $p < 11$. So $p = 7$, ind $x_3 = 39$, det $x_3 = -1$. There are no solutions.

So now assume x_1, x_2 are not reflections. If det $x_2 = \pm 1$, then ind $x_2 \geqslant \frac{3}{4}[(p^2-1)/p^2]\,n$. Since ind $x_1 \geqslant \frac{1}{2}[(p^2-1)/p^2]\,n$, this implies

$$\left(\frac{d_3-1}{d_3}\right)\left(\frac{p-1}{p}\right) n \leqslant \text{ind } x_3 < \left(2 - \frac{5}{4}\left(\frac{p^2-1}{p^2}\right)\right) n.$$

Thus $d_3 = 5$ and $p \leqslant 17$. However, then det $x_3 = 1$ and so ind $x_3 \geqslant \frac{4}{5}[(p^2-1)/p^2]\,n$. Then Σ ind $x_i > 2n$. If det x_2 has order 4, then

$$\frac{\text{ind } x_2}{n} \geqslant \frac{\frac{1}{2}(p-1) + \frac{3}{4}(p^2-p)}{p^2}.$$

Also $4 \mid d_3$ and so $d_3 \geqslant 8$. Moreover, $p \equiv 1 \bmod 4$. The only possibility (using Lemma 3.4) is that $p = 13$ and $d_3 = 8$. However, then ind $x_3 \geqslant \frac{147}{169}n$ and Σ ind $x_i > 2n$.

(5.5) If $d_3 \geqslant d_2 > 4$, Theorem 5.1 holds.

Proof. By Lemma 3.4, $2 > (1/n)\,\Sigma \text{ ind } x_i \geqslant (\frac{1}{2}+\frac{8}{5})(1-p^{-1})$. This implies $p \leqslant 19$. Moreover, if $p \geqslant 17$, a similar computation shows that $d_2 = d_3 = 5$ and $p = 17$. Then

$$\text{ind } x_i \geqslant \frac{4}{5}\left(\frac{17^4-1}{17^4}\right) n, \qquad i > 1,$$

and $\Sigma \operatorname{ind} x_i > 2n$. Similarly, if $p = 13$, $d_2 = 5$, and $d_3 \leqslant 7$. Then

$$\operatorname{ind} x_2 \geqslant \frac{4}{5}\left(\frac{13^4 - 1}{13^4}\right), \qquad \operatorname{ind} x_3 \geqslant \frac{10}{13} n,$$

and $\Sigma \operatorname{ind} x_i > 2n$. If $p = 11$ and neither x_2 nor x_3 is a reflection, then for $j > 1$

$$\operatorname{ind} x_j \geqslant \frac{96}{121} n,$$

and $\Sigma \operatorname{ind} x_i > 2n$. If say x_2 is a reflection, then by Lemma 3.5, $[x_1, N] = N$, and so x_1 acts as a scalar on N. This contradicts the irreducibility of G on N.

So assume $p = 7$. As above x_j is not a reflection for $j > 1$. Thus for $j > 1$, $\operatorname{ind} x_j \geqslant \frac{36}{49} n$ and if $d_j > 7$, $\operatorname{ind} x_j \geqslant \frac{291}{343} n$. Thus $d_j \leqslant 7$. If $d_3 = 7$, then $\Sigma \operatorname{ind} x_i \geqslant 2n$ unless $f(x_3) > 0$ and x_3 acts as a transvection. Then $e = 2$ and so x_1 must be a reflection. Since $G = \langle x_1, x_3 \rangle$, this contradicts Lemma 3.5. So assume $d_j \leqslant 6$ for $j = 2, 3$. Then as x_j is not a reflection, $\operatorname{ind} x_j \geqslant \frac{37}{49} n$. Thus $\operatorname{ind} x_1 < \frac{24}{49} n$, and so x_1 is a reflection. Thus $\det x_2 x_3 = -1$ and so we can assume d_3 is even. Thus $d_3 = 6$. If $d_2 = 5$, then $\det x_2 = 1$ and $\det x_3 = -1$. Thus $\operatorname{ind} x_3 \geqslant \frac{39}{49} n$ and $\Sigma \operatorname{ind} x_i \geqslant 2n$. The same argument applies when $d_2 = 6$ unless x_j^2 is a reflection for $j = 2$ or 3. If this is the case, then $e = 2$ (as $[x_j, N] = N$ and $\langle x_j, x_j \rangle$ acts irreducibly). Then we assume x_j^2 is a reflection for $j = 2, 3$ so say $\det x_2^3 = 1$. Then $\operatorname{ind} x_2 = 38$, $\operatorname{ind} x_3 = 37$, and $\Sigma \operatorname{ind} x_i = 2n - 2$. By inspection, one verifies that $\langle x_1, x_2 \rangle$ does not act irreducibly.

6. The Case $p = 5$

Recall we have found all examples with $r > 3$ for $p = 5$ in Section 4. Thus we assume $G = \langle x_1, x_2, x_3 \rangle$ with $x_1 x_2 x_3 = 1$, x_i of order $d_i > 1$, and $N = F(G) = O_5(G'') \neq 1$. Moreover, we assume that G acts primitively and faithfully on a set Ω with $|\Omega| = n = 5^e$. For the sake of brevity, we will only prove:

THEOREM 6.1. *If* $\Sigma \operatorname{ind} x_i = 2n - 2$, *then* $e \leqslant 3$.

In fact, the complete result is:

THEOREM 6.2. *If* $\Sigma \operatorname{ind} x_i = 2n - 2$, *then* (*up to permutation*) *one of the following holds*:

(a) $e = 3$ *and* $(d_1, d_2, d_3) = (2, 3, 8)$ *with* $G/N \cong C_4^2 \cdot S_3$,

(b) $e=2$ *and* $(d_1, d_2, d_3)=$

(i) $(2, 3, 10)$ *with* $G/N \cong S_3$,

(ii) $(2, 4, 8)$ *with* $G/N \cong T \in Syl_2(GL_2(5))$,

(iii) $(3, 4, 4)$ *with* G/N, *isomorphic to the normalizer (in* $GL_2(5)$*) of a Sylow 2-subgroup of* $SL_2(5)$.

(iv) $(2, 3, 12)$ *with* $|G/N|=96$,

(v) $(2, 3, 20)$ *with* $[G/N:SL_2(5)]=2$.

In order to give the reader a feeling for how one determines the groups that do exist, we shall give the details for case (a) of Theorem 6.2.

EXAMPLE 6.3. We wish to produce $h_i \in GL_3(5)$ of order d_i, $i=1, 2, 3$, such that

(i) $h_1h_2h_3=1$,

(ii) $\det h_i=1$ for each i,

(iii) $H=\langle h_1, h_2\rangle$ acts irreducibly on N, the natural module, and

(iv) $(d_1, d_2, d_3)=(2, 3, 8)$.

Now choose a basis $\{e_1, e_2, e_3\}$ for N such that $\{e_1, e_2\}$ spans the -1 eigenspace of h_1 and $h_2e_3=e_3$. Thus,

$$h_1=\begin{pmatrix}-1 & 0 & a\\ 0 & -1 & b\\ 0 & 0 & 1\end{pmatrix}, \qquad h_2=\begin{pmatrix}s & t & 0\\ u & v & 0\\ c & d & 1\end{pmatrix}, \qquad \theta=\begin{pmatrix}s & t\\ u & v\end{pmatrix},$$

where $1 \neq \theta^3=1$. The irreducibility is equivalent to $(a, b) \neq (0, 0) \neq (c, d)$. By conjugating by a block diagonal matrix, we may assume that

$$h_2=\begin{pmatrix}0 & -1 & 0\\ 1 & -1 & 0\\ 0 & 1 & 1\end{pmatrix}, \qquad h_1h_2=\begin{pmatrix}0 & 1+a & a\\ -1 & 1+b & b\\ 0 & 1 & 1\end{pmatrix}.$$

Note that the above conditions determine two possible conjugacy classes for h_3. Fix one choice. Then b is determined by the trace of h_3, and a is determined by the fact that the trace of h_3 is an eigenvalue of h_3. For example, if we wish h_3 to have trace 3 (the other possibility is trace 2), then h_1h_2 has trace 2, whence $b=0$. Since 2 is an eigenvalue of h_1, h_2, $a=1$. Thus up to conjugation in $GL_3(3)$, there is a unique such triple.

Now we observe that

$$h_1'=\begin{pmatrix}0 & 2 & 0\\ 3 & 0 & 0\\ 0 & 0 & -1\end{pmatrix}, \qquad h_2'=\begin{pmatrix}0 & 0 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix},$$

and $h_3' = (h_1' h_2')^{-1}$ also satisfy the conditions, and clearly generate $C_4^2 \cdot S_3 = H$. Note also that Σ ind $h_i = 248$, where ind is computed with respect to the permutation action on N. Set $G = NH$. By Proposition 3.6, there exist $x_i \in G$ conjugate to h_i with $G = \langle x_1, x_2, x_3 \rangle$ and $x_1 x_2 x_3 = 1$.

LEMMA 6.4. *Let $x \in G$ be of order d.*

(a) *If $d = 6$ or 10, then* ind $x \geqslant \frac{98}{125} n$. *Moreover, if* ind $x \neq \frac{98}{125} n$, *then* ind $x \geqslant \frac{4}{5} n$.

(b) *If $d > 6$ and $8 \neq d \neq 10$,* ind $x \geqslant \frac{534}{625} n$.

(c) *If $d = 5$,* ind $x \geqslant \frac{16}{25} n$. *If $f(x) = 0$, ind $x = \frac{4}{5} n$.*

(d) *If $d = 4$, then one of the following holds:*

(i) *x is a reflection and* ind $x = \frac{3}{5} n$,

(ii) *x is not a reflection, x^2 is a reflection, and* ind $x \geqslant \frac{17}{25} n$,

(iii) *x^2 is not a reflection, and* ind $x \geqslant \frac{18}{25} n$.

Moreover, if $f(x) > 0$ and $|[x, N]| > 5$, then ind $x \geqslant \frac{96}{125} n$:

(e) *If $d = 3$, then* ind $x \geqslant \frac{16}{25} n$.

(f) *If $d = 8$, then either ind $x = \frac{21}{25} n$ and $|[x, N]| = 25$ or ind $x \geqslant \frac{534}{625} n$.*

Proof. These follow from the results in Sections 2 and 3. For (b), note that it suffices to verify the inequality for $d = 9, 12, 15, 16, 20, 25$, and a prime larger than 5.

We assume for the rest of the section that $d_1 \leqslant d_2 \leqslant d_3$ and Σ ind $x_i = 2n - 2$.

(6.5) If $d_1 > 2$, $e < 4$.

Proof. By (6.4), $d_3 \geqslant 6$ implies ind $x_3 \geqslant \frac{98}{125} n$. By Lemma 3.5, there is at most one reflection among the x_i. So $d_3 \geqslant 6$ implies that Σ ind $x_i \geqslant [\frac{98}{125} + \frac{3}{5} + \frac{16}{25}] n > 2n$. If $d_3 = 5$ and x_3 is not a transvection (with $f(x_3) > 0$), then ind $x_3 \geqslant \frac{96}{125} n$ and, as above, Σ ind $x_i > 2n$.

So consider the case $d_3 = 5$ and x_3 is a transvection. If $d_1 = 3$, then $e \leqslant 3$. If $d_2 = 5$, then, as above, x_2 is a transvection whence $e \leqslant 2$. So $d_1 = d_2 = 4$. If $e > 3$, then $|[x_i, N]| \geqslant 125$ for $i < 3$. Then Σ ind $x_i \geqslant ((2 \cdot 87)/125 + (16/25)) n > 2n$.

Thus $d_3 < 5$, and so $d_3 = 4$. If $d_1 = d_2 = 3$, then det $x_3 = 1$ and ind $x_3 \geqslant \frac{18}{25} n$ by Lemma 3.3. Thus Σ ind $x_i \geqslant 2n$. So $d_2 = 4$. If $d_1 = 3$, then x_2 or x_3 a reflection implies $e \leqslant 3$. Then (6.4) implies Σ ind $x_i \geqslant 2n$. If $d_1 = 4$, then as at most one x_i is a reflection and some x_i satisfies det $x_i^2 = 1$, it follows from (6.4) that Σ ind $x_i \geqslant 2n$.

(6.6) *If $d_2 = 3$, $e < 4$.*

Proof. Note $\det x_2 = 1$. Thus $\det x_1 = \det x_3$. If x_1 is a reflection, then $e \leqslant 3$. Consider the case $|[x_1, N]| = 25$. Then $\det x_1 = \det x_3 = 1$. Also $|C_N(x_2)| \leqslant 3$ by Lemma 3.5. If $e > 5$, then $\langle x_1, x_2 \rangle$ fixes a plane. If $e = 4$ or 5, then $\operatorname{ind} x_1 = \frac{12}{25}n$, $\operatorname{ind} x_2 = \frac{416}{625}n$, and so $\operatorname{ind} x_3 = \frac{534}{625}n - 2$. Since $e < 6$, $d_3 \neq 7$. So $d_3 > 7$. If $d_3 \neq 8$ or 10, then $\operatorname{ind} x_3 \geqslant \frac{534}{625}n$. If $d_3 = 8$ or 10, one checks directly that the above equality cannot hold.

So $|[x_1, N]| > 25$. Thus $\operatorname{ind} x_1 \geqslant \frac{62}{125}n$. If $e > 3$, $|[x_2, N]| > 25$ or $\langle x_1, x_2 \rangle$ leaves a line invariant. Thus $\operatorname{ind} x_2 \geqslant \frac{416}{625}n$, and so $\operatorname{ind} x_3 \leqslant \frac{534}{625}n - 2$. As above this implies $d_3 = 8$ or 10. If $d_3 = 8$, then $|[x_3, N]| = 25$. Thus $e < 4$ by Lemma 3.5. So $d_3 = 10$. Note $[x_1, N]$ does not contain a hyperplane (by irreducibility). Thus $\operatorname{ind} x_1 \equiv 0 \bmod 25$. Also $\operatorname{ind} x_2 \equiv 5$ or 16 mod 25. Thus $\operatorname{ind} x_3 \equiv 23$, 18, or 7 mod 25. Hence $f(x_3) \leqslant 5$. If x_3^2 is not a transvection, then $\operatorname{ind} x_3 \geqslant \frac{534}{625}n$. Thus the -1 eigenspace of x_3 has codimension at most 2 and so must intersect $[x_1, N]$, a contradiction.

(6.7) If $d_2 = 4$, $e < 4$.

Proof. If x_1 is a reflection, $[x_2, N] = N$, and x_2 has distinct eigenvalues. Thus $e < 4$. Clearly, x_2 is not a reflection. If $|[x_2, N]| = 25$, then Lemma 3.5 implies $|[x_1, N]| \geqslant 5^{e-1}$. Then $C_N(x_2) \cap [x_1, N] \neq 1$, which contradicts the irreducibility of N. So $|[x_2, N]| \geqslant 125$. This implies that $\operatorname{ind} x_3 \leqslant \frac{103}{125}n - 2$. Thus $d_3 = 5$ or 10. In particular, $\det x_2^2 = 1$. Thus $\operatorname{ind} x_2 \geqslant \frac{92}{125}n$, and so $\operatorname{ind} x_3 \leqslant \frac{98}{125}n - 2$. Thus $d_3 = 5$, $f(x_3) > 0$, and $|[x_3, N]| \leqslant 25$, whence $e \leqslant 4$. Since $[x_1, N] \cap C_N(x_3) = 1$, $|[x_1, N]| = 25 = |[x_3, N]|$. By Proposition 3.6, $[x_1, N] \cap [x_3, N] \neq 1$, whence $[x_1, N][x_3, N]$ is a proper invariant subgroup of N.

Now assume $d_2 > 4$ and $e > 3$.

(6.8) x_2 is not a transvection.

Proof. If so, then $e \leqslant 2$.

(6.9) x_1 is a reflection.

Proof. Since x_2 and x_3 are not transvections, $\operatorname{ind} x_j \geqslant \frac{96}{125}n$ for $j > 1$. Thus $\operatorname{ind} x_1 < \frac{58}{125}n$, and so x_1 is a reflection.

(6.10) $d_2 \neq 5$.

Proof. If $d_2 = 5$, then $f(x_2) > 0$ implies $[x_2, N] = N$ by Lemma 3.5. This is impossible. So $f(x_2) = 0$ and $\operatorname{ind} x_2 = \frac{4}{5}n$. Thus $\operatorname{ind} x_3 = \frac{4}{5}n - 2$ and $\det x_3 = -1$. This implies $d_3 = 6$ or 10. If $f(x_3) = 0$, this implies $\Sigma \operatorname{ind} x_i > 2n$. Otherwise, Lemma 3.5 implies $[x_3, N] = N$. Since x_3 has no two-dimensional eigenspace, this implies $e < 4$ if $d_3 = 6$ and $\operatorname{ind} x_3 \geqslant \frac{4}{5}n$ if $d_3 = 10$.

(6.11) $d_2 \neq 6$.

Proof. If $d_2 = 6$, $[x_2, N] = N$ by (6.9) and Lemma 3.6. As x_2 has no two-dimensional eigenspace (over the algebraic closure), $e > 3$ implies $\operatorname{ind} x_2 \geqslant \frac{516}{625}n$. Thus $\operatorname{ind} x_3 < \frac{484}{625}n < \frac{98}{125}n$, a contradiction, as $d_3 \geqslant 6$.

(6.12) $d_2 \leqslant 6$.

Proof. Assume $d_2 > 6$. If d_2 or $d_3 = 8$ and $\operatorname{ind} x_i < \frac{534}{625}n$, then by Lemma 3.5, $e < 4$. So either $d_2 = d_3 = 10$ or $\Sigma \operatorname{ind} x_i \geqslant \frac{2}{5}n + \frac{98}{125}n + \frac{534}{625}n > 2n$. So assume $d_2 = d_3 = 10$. We can assume $\operatorname{ind} x_2 \geqslant \frac{4}{5}n$. Thus $\operatorname{ind} x_2 = \frac{98}{125}n$ and $|[x_2, N]| = 25$. Hence $|N| \leqslant |[x_1, N][x_2, N]| \leqslant 125$.

7. The Case $p = 3$

In this section, we assume the hypotheses of Section 4. We also assume that $O_3(G'') \neq 1$. As usual, we also assume that $d_1 \leqslant \cdots \leqslant d_r$. We first record some properties of $\operatorname{ind} x$ in this case.

(7.1) Suppose $x \in G$ has order d.

(a) If $d = 4$, $\operatorname{ind} x \geqslant \frac{2}{3}n$. If $|[x, N]| \geqslant 81$, $\operatorname{ind} x \geqslant \frac{58}{81}n$.

(b) If $d = 5$ or $d > 6$, $\operatorname{ind} x \geqslant \frac{7}{9}n$.

(c) If $d = 6$, $\operatorname{ind} x \geqslant \frac{17}{27}n$.

(d) If $d > 9$ and $d \neq 12$, $\operatorname{ind} x \geqslant \frac{209}{243}n$.

By the results of Section 4, it suffices to assume $r = 3$ or 4. First consider the case $r = 4$.

(7.2) If $r = 4$, then $e \leqslant 6$.

Proof. Since $G'' \neq 1$, $d_4 > 2$. If x_1, x_2, and x_3 are reflections, then $e \leqslant 2$ by Lemma 3.2. If say x_1 and x_2 are reflections, then $\operatorname{ind} x_3 + \operatorname{ind} x_4 = \frac{4}{3}n - 2$. Thus $\operatorname{ind} x_j < \frac{2}{3}n$ for $j = 3$ or 4. For this j, $d_j = 2$, 3, or 6. If $d_3 = 2$, then Lemma 3.5 implies $[x_3, N]$ contains a hyperplane. Thus for $e > 3$, $C_N(x_1) \cap C_N(x_2) \cap [x_3, N]$ is a nontrivial normal subgroup of G. If $d_3 = 3$, then as $C_N(x_1) \cap C_N(x_2) \cap C_N(x_3) = 1$, it follows that $|C_N(x_3)| \leqslant 9$. Thus $e \leqslant 6$. If $d_3 > 3$, then either d_3 or $d_4 = 6$. Suppose $d_3 = 6$ and $\operatorname{ind} x_3 < \frac{2}{3}n$. Then $f(x_3) > 0$, and so Lemma 3.5 implies $[x_3, N]$ contains a hyperplane. For $e \geqslant 4$, this implies $\operatorname{ind} x_3 \geqslant \frac{2}{3}n$. If $\operatorname{ind} x_3 \geqslant \frac{2}{3}n$, then $d_4 = 6$, and the above argument applies to x_4. If x_1 is the unique reflection, then $\operatorname{ind} x_j \geqslant \frac{4}{9}n$ for $j > 1$. Thus $\operatorname{ind} x_j < \frac{7}{9}n$ for each j. Hence $d_j < 7$ and $d_j \neq 5$. Similarly, at most one d_j is 4 or 6. If x_2 acts as a scalar on N, then as $d_3 < 4$, $\langle x_1, x_2, x_3 \rangle$ has an invariant line on N for $e > 3$. Otherwise, $\operatorname{ind} x_i \equiv 0 \bmod 3$ for $i < 4$. Thus $\operatorname{ind} x_4 \equiv 1 \bmod 3$, and so $\operatorname{ind} x_4 \geqslant \frac{13}{18}n - \frac{1}{2}$. Thus $\operatorname{ind} x_2 + \operatorname{ind} x_3 < \frac{17}{18}n$. If $d_2 = d_3 = 2$, this implies $|[x_2, N]| = 9$ and so $e \leqslant 6$. If $d_3 = 3$, then $|[x_3, N]| = 3$, and again $e < 6$. Finally, assume that no x_i is a reflection.

Then ind $x_i \geqslant \frac{4}{9}n$ for each i. So ind $x_i < \frac{2}{3}n$ for each i. This implies ind $x_1 \equiv 0$ mod 3 unless $d_i = 2$ and x_i acts as a scalar on N. So assume $d_1 = 2$ and $[x_1, N] = N$. Since $\langle x_i, x_j \rangle$ acts irreducibly on N for $i, j > 1$, it follows that $|[x_i, N]|\,|[x_j, N]| \geqslant n$. Case analysis shows that Σ ind $x_i \geqslant 2n$.

For the rest of the section, we take $r = 3$.

(7.3) If $d_1 > 2$, then $e \leqslant 6$.

Proof. Since ind x_2 + ind $x_3 < \frac{14}{9}n$, it follows that $d_2 \leqslant 6$. Thus if x_1 is a transvection, $e \leqslant 6$. If $d_3 = 5$ or $d_3 > 6$, then ind x_1 + ind $x_2 < \frac{11}{9}n$. Since ind $x_i \geqslant \frac{16}{27}n$, this implies ind $x_i < \frac{17}{27}n$ for $i = 1, 2$. This implies $d_1 = d_2 = 3$ and $|[x_i, N]| \leqslant 9$ for $i = 1, 2$, whence $e \leqslant 3$. So $d_i = 3, 4$, or 6. Since $N = [x_1, N][x_2, N]$, $|[x_i, N]| \geqslant 81$ for $i = 1$ or 2. If $d_1 = d_2 = 3$, this implies ind $x_3 \geqslant \frac{13}{18}n - \frac{1}{2}$ and Σ ind $x_i > 2n$. If $d_1 = 3$, and $d_2 > 3$, then $|[x_2, N]| \geqslant 27$. Thus ind $x_2 \geqslant \frac{19}{27}n$. Moreover, since ind x_2 or ind $x_3 \not\equiv 0$ mod 3, this implies Σ ind $x_i \geqslant 2n$. If $d_1 > 3$, the same argument applies (perhaps interchanging x_1 and x_2).

(7.4) *If* $(d_1, d_2) = (2, 3)$, then $e \leqslant 6$.

Proof. Since $G'' \neq 1$, $d_3 > 6$. If $e > 6$, then as $N = [x_1, N][x_2, N] = [x_2, N][x_2, N]^{x_1}$, it follows that $|[x_1, N]| \geqslant 27$ and $|[x_2, N]| \geqslant 81$. Thus ind $x_1 \geqslant \frac{13}{27}n$ and ind $x_2 \geqslant \frac{160}{243}n$. Thus ind $x_3 < \frac{209}{243}n$, and so $d_3 = 7, 8, 9$, or 12. Moreover, as $[x_1, N] \neq N$ (by irreducibility), ind $x_3 \equiv 1$ mod 3. This implies in each possible case that ind $x_3 > \frac{209}{243}n$.

(7.5) If $d_1, d_2, d_3) = (2, 4, 6)$, $e \leqslant 6$.

Proof. Assume $e > 6$. We consider several cases.

(a) If x_1 is a reflection, then $e \leqslant 3$.

(b) If $|[x_1, N]| = 9$, then no eigenvalue of x_2 occurs with multiplicity greater than 2 (over the algebraic closure). Moreover, by Lemma 3.2, $[x_2, N]$ contains a hyperplane. Thus $e \leqslant 7$. For $e = 7$,

$$\text{ind } x_2 = \frac{3}{4}(n - 81) + \frac{1}{2}\left(\frac{n}{81} - 3\right).$$

Hence ind $x_3 \equiv 13$ mod 27. This implies $\det x_3 = -1$. However, $\det x_1 \det x_2 = 1$, a contradiction.

(c) If $|[x_1, N]| \geqslant 27$, then ind $x_1 \geqslant \frac{13}{27}n$. Also $|C_N(x_1)| \geqslant 9$ (or $\langle x_1, x_2 \rangle$ has an invariant line over the algebraic closure). Thus ind $x_1 \equiv 0$ mod 9. If ind $x_3 \not\equiv 0$ mod 3, then, as no eigenspace of x_3 has dimension $> e/2$, ind $x_3 \geqslant \frac{133}{162}n - \frac{11}{2}$. Since ind $x_3 \not\equiv 7$ mod 9, ind $x_2 \not\equiv 0$ mod 9. This implies ind $x \geqslant \frac{526}{729}n$ and Σ ind $x_i > 2n$. So ind $x_3 \equiv 0$ mod 3, whence

ind $x_2 \equiv 1 \bmod 3$. This implies ind $x_2 \equiv 4 \bmod 9$, and so ind $x_3 \equiv 3 \bmod 9$. Then ind $x_2 \geqslant (1 - 554/3^7)\, n$ and ind $x_3 \geqslant \frac{13}{18}n - \frac{3}{2}$, whence Σ ind $x_i > 2n$.

(7.6) If $(d_1, d_2) = (2, 4)$, $e \leqslant 6$.

Proof. Assume $e > 6$.

(a) If x_1 is a reflection, then $e \leqslant 3$.

(b) If $|[x_1, N]| = 9$, ind $x_1 = \frac{4}{9}n$ and in x_2 is an in (7.5b). Then ind $x_3 = \frac{131}{162}n - \frac{1}{2} < \frac{22}{27}n$. Thus $d_3 = 5$, 8, 9, or 10. Moreover, as ind $x_3 \equiv 4 \bmod 9$, for $d_3 \neq 9$, $[x_3, N] = N$ and ind $x_3 \geqslant \frac{22}{27}n$. Similarly, if $d_3 = 9$, x_3 has exactly one Jordan block, and so ind $x_3 = \frac{8}{9}n - 8 > \frac{22}{27}n$ (since $e > 6$).

(c) If $|[x_1, N]| \geqslant 27$, then ind $x_1 \geqslant \frac{13}{27}n$. As $|[x_2, N]| \geqslant 81$, ind $x_2 \geqslant \frac{58}{81}n$. Thus ind $x_3 < \frac{65}{81}n$. Thus $d_3 \leqslant 9$ and $d_3 \neq 7$. Moreover, as $|[x_3, N]| \geqslant 81$, ind $x_3 < \frac{65}{81}n$ implies $d_3 \leqslant 6$. So we can assume $d_3 = 5$. Thus

$$\text{ind } x_1 = \tfrac{1}{2}(n - 3^a),$$
$$\text{ind } x_2 = \tfrac{3}{4}n - \tfrac{1}{4}3^b - \tfrac{1}{2}3^c,$$
$$\text{ind } x_3 = \tfrac{4}{5}(n - 3^d),$$

where $a = \dim C_N(x_1)$, $b = \dim C_N(x_2^2)$, $c = \dim C_N(x_2)$, and $d = \dim C_N(x_3)$. Since Σ ind $x_i = 2n - 2 \equiv -2 \bmod n$, it follows that $c = 0$ and $d = 1$. Since $b \leqslant a$ (as $C_N(x_2^2) \cap [x_1, N] = 1$), $\frac{1}{2} + \frac{12}{5} \equiv 2 \pmod{3^b}$, and so $b \leqslant 3$. Then Σ ind $x_i > 2n$.

(7.7) If $(d_1, d_2) = (2, 5)$, $e \leqslant 6$.

Proof. If x_1 is a reflection, $e \leqslant 5$. Otherwise ind $x_1 \geqslant \frac{4}{9}n$. Also ind $x_2 \geqslant \frac{64}{81}n$. Thus ind $x_3 < \frac{62}{81}n$ and so $d_3 = 6$. Since ind $x_1 \equiv 0 \bmod 9$ (or $\langle x_1, x_2 \rangle$ has an invariant subspace of dimension at most 5), it follows that ind $x_2 +$ ind $x_3 \equiv 7 \bmod 9$. If $f(x_3) = 0$, ind $x_3 \geqslant \frac{7}{9}n$, a contradiction. Since ind $x_2 = \frac{4}{5}(n - 3^a)$, it follows that either $a = 0$ and ind $x_3 \equiv 6 \bmod 9$ or $a = 1$ and ind $x_3 \equiv 4 \bmod 9$. In the first case, ind $x_2 = \frac{4}{5}(n - 1)$ and ind $x_3 \geqslant \frac{13}{18}n - \frac{15}{2}$. Then Σ ind $x_i > 2n$. In the latter case, Σ ind $x_i \not\equiv -2 \bmod 27$.

(7.8) If $(d_1, d_2) = (2, 6)$, then $e \leqslant 6$.

Proof. If x_1 is a reflection, then $e \leqslant 6$. So we can assume $|[x_1, N]| \geqslant 9$ (and similarly $|C_N(x_1)| \geqslant 9$). Then ind $x_1 \geqslant \frac{4}{9}n$ and ind $x_1 \equiv 0 \bmod 9$. We record some inequalities. They all follow from

$$\text{ind } x_2 = \tfrac{5}{6}n - \tfrac{1}{6}(2f(x_2) + 2f(x_2^2) + f(x_2^3))$$

and the fact that no eigenspace of x_2 has codimension at least $e/2$ (so $e > 6$ implies at least codimension at least 4). Hence

(i) if ind $x_2 \equiv 1 \bmod 3$, then ind $x_2 \equiv 4 \bmod 9$ and ind $x_2 \geqslant \frac{403}{486}n - \frac{1}{2}$,

(ii) if ind $x_2 \equiv 2 \bmod 3$, then ind $x_2 \geqslant \frac{403}{486}n - \frac{11}{2}$,

(iii) if ind $x_2 \equiv \pm 3 \bmod 9$, then, ind $x_2 \geqslant \frac{43}{54}n - \frac{33}{2}$.

First consider $d_3 = 6$. The above computations also apply to x_3. Since ind x_2 + ind $x_3 \equiv 7 \bmod 9$, it follows that

$$\Sigma \text{ ind } x_i \geqslant \tfrac{4}{9}n + \tfrac{403}{486}n + \tfrac{43}{54}n - 17 > 2n.$$

So $d_3 > 6$. Thus ind $x_3 \geqslant \frac{7}{9}n$, and so ind $x_2 < \frac{7}{9}n$. This implies ind $x_2 \equiv 0 \bmod 9$, and ind $x_3 \equiv 7 \bmod 9$. Note that $|[x_2, N]| \geqslant 81$. This implies ind $x_2 \geqslant \frac{173}{243}n$. Hence ind $x_3 < \frac{205}{243}n$. By case analysis, this cannot occur for $d_3 > 6$ and ind $x_3 \equiv 7 \bmod 9$.

(7.9) $e \leqslant 6$.

Proof. We can assume $d_1 = 2$ and $6 < d_2 \leqslant d_3$. Thus ind $x_j > \frac{7}{9}n$ for $j > 1$. Hence ind $x_1 < \frac{4}{9}n$. So x_1 is a reflection. One of $x_j, j > 1$, must satisfy ind $x_j < \frac{5}{6}n$. This implies for $j = 2$ or 3, $d_j = 8$, 9, or 12 and x_j has no multiple eigenvalues. If $d_j = 8$, this implies ind $x_j \geqslant \frac{5}{6}n$. If $d_j = 9$, this implies, x_j has a single Jordan block on N. Since $e > 6$, ind $x_j > \frac{5}{6}n$. A similar analysis shows ind $x_j \geqslant \frac{5}{6}n$ for $d_j = 12$.

8. The Case $p = 2$

We assume the usual notation and hypotheses. Also $N = O_2(G'') \neq 1$ with $|N| = n = 2^e$, $e > 16$.

(8.1) If $x \in G$ has order d, one of the following holds:

(a) ind $x \geqslant \frac{3}{4}n$,

(b) $d \leqslant 4$, or

(c) $d = 6$, $f(x) > 0$ with $|[x^3, N]| = 2$ or $|[x^2, N]| = 4$.

Proof. If d is divisible by an odd prime other than 3 or by 9, then (a) holds by Lemma 3.3. If d is a multiple of 8 or 12, (a) holds by inspection. If $d = 6$, then

$$\text{ind } x = \tfrac{5}{6}n - \tfrac{1}{3}f(x) - \tfrac{1}{3}f(x^2) - \tfrac{1}{6}f(x^3).$$

If $f(x) = 0$, then $f(x^3) = 0$ and since $f(x^2) \leqslant n/4$, (a) holds. If $|[x^3, N]| > 2$, then $f(x^3) \leqslant n/4$ and $f(x) \leqslant n/16$. If $|[x^2, N]| \neq 4$, then $f(x^2) \leqslant n/16$. Thus ind $x \geqslant \frac{3}{4}n$.

(8.2) Let x be in G of order d.

(a) If $d = 2$ or 4, ind $x \equiv 0 \bmod 8$.

(b) If $d=3$, ind $x \equiv 0 \bmod 4$ or ind $x = \frac{2}{3}(n-1)$. Moreover, ind $x \equiv 4 \bmod 8$ implies ind $x = \frac{2}{3}(n-2)$.

(c) If $d=5$, ind $x \equiv 0 \bmod 4$.

(d) If $d=6$, ind $x \geqslant \frac{3}{4}n-4$ or ind $x \equiv 0 \bmod 8$.

Proof. The results of Section 3 imply (a), (b), and (c) easily. If $d=6$ and ind $x < \frac{3}{4}n$, then $f(x)>0$. By (8.1c), either $|[x^3, N]|=2$ or $|[x^2, N]|=4$. In the first case, $f(x) \geqslant 8$ implies ind $x \equiv 0 \bmod 8$. So $f(x) \leqslant 4$ whence $f(x^3) \leqslant 8$ and ind $x \geqslant \frac{3}{4}n-4$. In the second case, ind $x \equiv 0 \bmod 8$.

(8.3) Some x_i satisfies ind $x_i \geqslant \frac{3}{4}n-4$.

Proof. Otherwise as Σ ind $x_i \equiv 6 \bmod 8$, ind $x_i \not\equiv \bmod 4$ for some x_i. By (8.1) and (8.2), $d_i=3$ and ind $x_i = \frac{2}{3}(n-1) \equiv 2 \bmod 8$. Thus either

(i) $r=3$, $d_1=d_2=d_3=3$, or

(ii) ind $x_j \equiv 4 \bmod 8$ for some j.

If (i) holds, then $G''=1$ by Proposition 2.4. If (ii) holds, then either ind $x_j \geqslant \frac{3}{4}n-4$ or $d_i=d_j=3$ and ind $x_i = \frac{2}{3}(n-1)$ and ind $x_j = \frac{2}{3}(n-2)$ for some i, j. However, since $n-1$ and $n-2$ are not both divisible by 3, the latter situation cannot occur.

(8.4) $r \leqslant 4$.

Proof. Since ind $x_i \geqslant n/4$ for all i, $r \leqslant 7$ (without the assumption $e>16$; note $r=7$ does occur for $n=8$). Indeed since ind $x_i \geqslant \frac{3}{4}n-4$ for some i, $r \leqslant 6$. Note that either $d_i=2$ with $f(x_i)>0$ or ind $x_i \geqslant \frac{3}{8}n$. If $r=6$, this implies that five of the x_i must be transvections and so $e<5$. If $r=5$, as above, we can assume that x_4 and x_5 are not transvections. If x_3 is not a transvection as well, then ind x_1 + ind $x_2 \leqslant (2n-2)-\frac{3}{4}n+\frac{3}{4}n-4 = (n/2)+2$. This implies x_1 and x_2 are transvections. We can assume ind $x_5 \geqslant \frac{3}{4}n-4$. Thus ind x_3 + ind $x_4 \leqslant \frac{3}{4}n+2$. This implies $|[x_3, N]| = |[x_4, N]|=4$ with $f(x_3), f(x_4) \neq 0$. Thus $e<6$. So we can assume x_1, x_2, and x_3 are transvections and ind $x_5 \geqslant \frac{3}{4}n-4$. Thus ind $x_4 \leqslant (n/2)+2$. Hence $d_4 \leqslant 4$. Moreover, if $d_4 \neq 2$, then $|[x_4, N]| \leqslant 4$. In this case by Lemma 3.5, $e<5$. If $d_4=2$, then as $N = MM^{x_4}$, where $M = [x_1, N][x_2, N][x_3, N]$, $n \leqslant |M|^2 \leqslant 64$.

(8.5) $r=3$.

Proof. By (8.4), it suffices to assume $r=4$. By (8.1), at most one $d_i>6$. Thus if two of the x_i's are transvections, $e \leqslant 12$.

If $d_i>2$ for each $i>1$, then ind $x_1 \leqslant (2n-2)-(\frac{3}{4}n-4+n) = (n/4)+2$. Thus x_1 is a transvection and ind $x_1 = n/4$. Moreover, since ind $x_i > n/2$

implies ind $x_i \geqslant \frac{9}{16}n$, it follows that (by reordering if necessary), ind $x_2 =$ ind $x_3 = n/2$ and ind $x_4 = \frac{3}{4}n - 2$. This implies $|[x_2, N]| = |[x_3, N]| = 4$ and so $e < 5$.

So assume $d_1 = d_2 = 2$ and ind $x_4 \geqslant \frac{3}{4}n - 4$. If $d_3 > 2$, ind $x_3 \geqslant \frac{1}{2}n$ and ind $x_1 +$ ind $x_2 \leqslant \frac{3}{4}n + 2$. Moreover, if ind $x_3 > \frac{1}{2}n$, then ind $x_3 \geqslant \frac{9}{16}n$, and ind $x_1 +$ ind $x_2 \leqslant \frac{11}{16}n + 2$. In this case $|[x_1, N]| = 2$ and $|[x_2, N]| \leqslant 8$ (or vice versa). If $|[x_2, N]| = 8$, then ind $x_2 = \frac{7}{16}n$ and so ind $x_3 \leqslant \frac{9}{16}n + 2$. Then $d_3 = 4$ and so $n \leqslant |[x_1, N][x_2, N]| \, 4 \leqslant 216$. If $|[x_2, N]| = 4$, then similarly ind $x_3 \leqslant \frac{5}{8}n + 2$. This implies $d_3 = 4$ (and $e \leqslant 12$ as above) or $d_3 = 6$. The latter implies $|[x_3, N]| \leqslant 8$ and so $e < 6$. If $|[x_2, N]| = 2$, then ind x_3 or ind $x_4 < \frac{3}{4}n$. So we can assume $d_3 \leqslant 6$. Thus $e \leqslant 12$.

Finally consider $d_1 = d_2 = d_3 = 2$. Let $e_i = \dim[x_i, N]$. Since $G = \langle x_1, x_2, x_3 \rangle$, it follows that for distinct $i, j \in \{1, 2, 3\}$, $2(e_i + e_j) \geqslant e > 16$. Since $e_i \leqslant e/2$ as well, it follows that

$$\frac{1}{n} \sum_{i=1}^{3} \text{ind } x_i \geqslant \sum_{i=1}^{3} \frac{1}{2}\left(1 - \frac{1}{2^{e_i}}\right) \geqslant \frac{43}{32},$$

unless one of the x_i is a transvection. Since ind $x_4 \geqslant \frac{3}{4}n - 2$, this is a contradiction. So assume x_1 is a transvection. Then, as above,

$$\frac{1}{n} \sum_{i=1}^{3} \text{ind } x_i \geqslant \frac{5}{4} - \frac{1}{256}.$$

Thus ind $x_4 < (\frac{3}{4} + \frac{1}{256})n$. This easily implies that $d_4 \leqslant 8$ or $d_4 = 10$, 12, or 14. Since ind $x_4 \equiv 14 \mod 16$, $d_4 \neq 2, 3, 4, 5, 7, 8$, or 10. If $d_4 = 14$ and ind $x_4 \not\equiv 0 \mod 4$, ind $x_4 \geqslant \frac{27}{32}n$. Similarly, if $d_4 = 12$, ind $x_4 \geqslant \frac{5}{6}n - \frac{28}{3}$. So $d_4 = 6$. Thus

$$\text{ind } x_4 = \tfrac{5}{6}n - \tfrac{1}{6}(2f(x_4) + 2f(x_4^2) + f(x_4^3)).$$

Since ind $x_4 \equiv 6 \mod 8$, it follows that $f(x_4) = 2$ and $f(x_4^2) = 4$. Thus ind $x_4 = \frac{5}{6}n - \frac{1}{6}f(x_4^3) - 2$. If $f(x_4^3) \neq n/2$, then ind $x_4 \geqslant \frac{19}{24}n - 2$, a contradiction. So ind $x_4 = \frac{3}{4}n - 2$. Since ind x_2, ind $x_3 \leqslant n/2$, we must have ind $x_2 =$ ind $x_3 = n/2$. Thus $f(x_2) = f(x_3) = 0$. Hence N cannot be projective as an $\langle x_2 \rangle$ or $\langle x_3 \rangle$ module. Thus $\dim[x_i, N] = e_i < e/2$ for $i = 2, 3$. Moreover, since e is even (by the action of x_4 on N), it follows that $[x_1, N][x_2, N][x_3, N] \neq N$, and so G does not act irreducibly on N.

We now assume that $d_1 \leqslant d_2, d_3$. Let $e_i = \dim[x_i, N]$.

(8.6) $d_1 = 2$.

Proof. Assume $d_1 > 2$. At most one x_i can satisfy ind $x_i \geqslant \frac{3}{4}n$. Thus the possibilities for (d_1, d_2, d_3) are:

(i) $(3, 3, d)$

(ii) $(3, 4, d)$

(iii) $(4, 4, d)$

(iv) $(3, 6, d)$

(v) $(4, 6, d)$

(vi) $(6, 6, d)$.

We can assume $\operatorname{ind} x_3 \geqslant \frac{3}{4}n - 4$. Also $\dim[x_i, N] = e_i$ must satisfy $6e_i \geqslant e > 16$. So $e_i > 2$. Thus for $d_i = 3$, $\operatorname{ind} x_i \geqslant \frac{5}{8}n$. If $d_2 < 6$, then in fact $4e_i > 16$. Thus $e_i > 4$. If $d_i = 3$, $\operatorname{ind} x_i \geqslant \frac{21}{32}n$. This eliminates case (i). If $d_i = 4$, then $e_i > 4$ implies $\operatorname{ind} x_i \geqslant \frac{43}{64}n$ unless x_i^2 is a transvection in which case $\operatorname{ind} x_i \geqslant \frac{39}{64}n$. This eliminates cases (ii) and (iii) unless $d_1 = d_2 = 4$ and x_i^2 is a transvection for $i = 1, 2$. Then $\operatorname{ind} x_3 \leqslant \frac{25}{32}n - 2$ and $\operatorname{ind} x_3 \equiv 6 \bmod 8$. Hence as in (8.5), $d_3 = 6$ and $\operatorname{ind} x_3 = \frac{3}{4}n - 2$. Since $\operatorname{ind} x_1$, $\operatorname{ind} x_2$ are most $\frac{5}{8}n$, this implies $\operatorname{ind} x_j = \frac{5}{8}n$ for $j = 1, 2$. Thus $f(x_1) = f(x_2) = 0$ and $f(x_3) = 2$. Since $f(x_i^2) = n/2$ for $i = 1, 2$ and $N = [x_1, N][x_2, N]$, it follows for $i = 1, 2$ that x_i has one Jordan block of size 3, one of size 1, and the rest of size 2. Let M be a subgroup of N, invariant under all transvections in G. Assume M is irreducible under the subgroup T of H generated by these transvections. Then $N = M_1 \oplus M_2 \oplus \cdots \oplus M_k$, where the M_i are the conjugates of M. Note that as $f(x_3^2) = 4$, x_3^2 must leave each M_i invariant. Since x_3^3 is a transvection, x_3 leaves each M_i invariant. Since x_1^2 is a transvection, x_1 must leave some M_i invariant. Thus as $G = \langle x_1, x_3 \rangle$, $M = N$. Write $x_i = h_i u_i$ with $h_i \in H$ and $u_i \in N$. Since $\operatorname{ind} h_i = \operatorname{ind} x_i - f(h_i)/2 \leqslant \operatorname{ind} x_i - 8$ for $i = 1, 2$, it follows that $\Sigma \operatorname{ind} h_i \leqslant 2n - 18$. Since $\Sigma \operatorname{ind} h_i \geqslant 2(n - l)$, where l is the number of orbits of H on N, $l \geqslant 9$. Thus by [Mc], $T \cong S_{e+1}$ or S_{e+2}. Since $T \lhd H$, $H = T$. However, in S_{e+1} or S_{e+2}, no transvection (transposition) is a square.

So assume $d_2 = 6$. If $d_1 \neq 6$, then $e_2 > 4$, and so $\operatorname{ind} x_2 \geqslant \frac{17}{24}n$. Thus $\operatorname{ind} x_1 \leqslant \frac{13}{24}n$ and so $e_1 < 3$, a contradiction. So assume $d_1 = 6$. Then $\operatorname{ind} x_1 = \operatorname{ind} x_2 = \frac{5}{8}n$ or $\Sigma \operatorname{ind} x_i \geqslant 2n$. This implies $e_1 = e_2 = 3$, and so $e \leqslant 6$.

For the rest of the section, we assume $d_1 = 2$. Let $e_i = \dim[x_i, N]$.

(8.7) $d_2 > 3$.

Proof. Assume $d_2 = 3$. Then $e_1 \geqslant 6$ and $e_2 \geqslant 9$. Thus $\operatorname{ind} x_1 \geqslant \frac{127}{256}n$ and $\operatorname{ind} x_2 \geqslant \frac{2}{3}(1 - 1/2^{10})n$. Hence $\operatorname{ind} x_3 < \frac{205}{256}n$. Since $d_3 > 6$, this implies $d_3 = 8$, 10, 12, or 14. Also $\operatorname{ind} x_3 \not\equiv 0 \bmod 8$. This rules out $d_3 = 8$. If $d_3 = 10$, the congruence condition implies $f(x_3) \leqslant 2$ and $f(x_3^2) \leqslant 4$, whence $\operatorname{ind} x_3 > \frac{205}{256}n$. A similar argument holds for $d_3 = 12$ or 14.

(8.8) $d_2 > 4$.

Proof. Assume $d_2 = 4$. Then $d_3 \geqslant 5$. Now $e_1 \geqslant 5$. So $\operatorname{ind} x_1 \geqslant \frac{31}{64}n$. Similarly $e_2 \geqslant 9$, and so $\operatorname{ind} x_2 \geqslant (5/8 - 1/2^{10})n$. As $\operatorname{ind} x_3 \equiv 14 \bmod 16$, $d_3 \neq 5, 7, 8, 9, 10, 11, 13, 14,$ or 17. Moreover, $d_3 = 15$ and $\operatorname{ind} x_3 \equiv 14 \bmod 16$ implies $\operatorname{ind} x_3 = \frac{14}{15}(n - 1)$, and so $\Sigma \operatorname{ind} x_i > 2n$.

Next consider $d_3 = 6$. Since ind $x_3 \equiv 14 \bmod 16$, $f(x_3) = 2$ and $f(x_3^2) = 4$. Thus ind $x_3 = \frac{5}{6}n - 2 - \frac{1}{6}f(x_3^3)$. Since $2n - 2 = \Sigma$ ind x_i, this implies

$$\frac{n}{12} = \frac{f(x_3^3)}{6} + \frac{f(x_2)}{2} + \frac{f(x_2^2)}{4} + \frac{f(x_1)}{2}.$$

Since $f(x_1) \leqslant n/2^9$ and $f(x_2) \leqslant n^{1/2}$, the only solution is $f(x_3^3) = n/2$ and $f(x_1) = f(x_2) = f(x_2^2) = 0$. Hence x_3^3 is a transvection. Let T be the subgroup of H generated by transvections. So $N = N_1 \oplus \cdots \oplus N_s$, where the N_i are the irreducible T-submodules of N. Note x_3 leaves N_1 invariant, where N_1 is the component on which x_3^3 acts nontrivially. Also since x_3 acts an element of order 3 on $M = N_2 \oplus \cdots \oplus N_s$ and $f(x_3) = 2$, x_3 cannot permute the N_i nontrivially. So x_3 normalizes each N_j. If x_1 did not fix any N_j, then $[x_1, N] = C_N(x_1)$ and so N is a projective $\langle x_1 \rangle$-module. Then any two elements of order 2 in $x_1 N$ are conjugate, and so $f(x_1) > 0$, a contradiction. Hence $\langle x_1, x_3 \rangle$ fixes some N_j, whence $N = N_j$ is an irreducible T-module. Write $x_i = h_i v_i$, $h_i \in H$, $v_i \in N$ for each i. Since Σ ind $h_i < \Sigma$ ind $x_i - |C_N(h_1)| \leqslant 2n - 10$, it follows that H has at least four orbits on N. Hence by [Mc], $H \cong S_{e+1}$ or S_{e+2}. Let $\sigma(x_i)$ be the index of x_i viewing it as an element in G/N acting on $f = e + 1$ or $e + 2$ points. Since x_3^3 is a transposition, it follows that $\sigma(x_3) \leqslant \frac{2}{3}f + \frac{1}{3}$. Thus, as $f > 14$, $\Sigma\sigma(x_i) < 2f - 2$. This contradicts the fact that $\langle x_1, x_2, x_3 \rangle$ acts transitively on the f points.

Next consider $d_3 = 12$. Since ind $x_3 \equiv 14 \bmod 16$, ind $x_3 \geqslant \frac{41}{48}n - 2$. Thus ind $x_2 \leqslant \frac{127}{192}n$. Since $f(x_2) \leqslant n^{1/2}$, it follows that $f(x_2^2) = n/2$. Thus,

$$\text{ind } x_1 = \frac{n}{2} - \frac{f(x_1)}{2}$$

$$\text{ind } x_2 = \frac{5}{8}n - \frac{f(x_2)}{2}$$

$$\text{ind } x_3 = \frac{11}{12}n - \frac{1}{12}[4f(x_3) + 2f(x_3^2) + 2f(x_3^3) + 2f(x_3^4) + f(x_3^6)].$$

By the congruence condition, either

(i) $f(x_3) = 2$, $f(x_3^2) = f(x_3^4) = 4$ or

(ii) $f(x_3) = 0$, $f(x_3^2) = 4$, and $f(x_3^4) = 8$.

In case (ii), one obtains

$$\frac{n}{8} = \frac{f(x_1)}{2} + \frac{f(x_2)}{2} + \frac{f(x_3^6)}{12}.$$

Since $f(x_1) \leqslant n/2^9$ and $f(x_2) \leqslant n^{1/2}$, this cannot be solved. In case (i), one obtains

$$6f(x_1) + 6f(x_2) + 2f(x_3^3) + f(x_3^6) = n/2.$$

Since $f(x_3) \neq 0$, $f(x_3^6) > f(x_3^3) > 0$, the only possible solutions (noting the bounds on $f(x_1)$ and $f(x_2)$) are with $f(x_1) = f(x_2) = 0$. Thus $f(x_3^3) = n/8$ and $f(x_3^6) = n/4$. However, by considering rational canonical forms, we see that no such element of order 12 exists.

So $d_3 \geqslant 18$. If x_2^2 is not a transvection, then $\operatorname{ind} x_2 \geqslant \frac{43}{64}n$ and so $\operatorname{ind} x_3 < \frac{7}{8}n$, a contradiction. If x_2^2 is a transvection, then $e_2 \leqslant e/2 + 1$. Hence as $e_1 + e_2 \geqslant e$, $e_1 \geqslant e/2 - 1$. Thus $\operatorname{ind} x_1 \geqslant \frac{1}{2}(n - 2^8)$, and so $\operatorname{ind} x_3 < (7/8 + 3/3^9)\, n$. This implies $d_3 = 21$ or 24. If $d_3 = 21$, $\operatorname{ind} x_3 \not\equiv 14 \bmod 16$. If $d_3 = 24$ and $\operatorname{ind} x_3 \equiv 14 \bmod 16$, then $f(x_3^8) \leqslant 2^8$, and $\operatorname{ind} x_3 \geqslant \frac{173}{192}n$, a contradiction.

(8.9) $d_2 > 5$.

Proof. Assume $d_2 = 5$. As $e_1 \geqslant 5$, $\operatorname{ind} x_1 \geqslant \frac{15}{32}n$. Also $e_2 \geqslant 9$ implies $\operatorname{ind} x_2 \geqslant \frac{4}{5}(1 - 1/2^{12})n$. Thus $\operatorname{ind} x_3 \leqslant (2n-2) - [\frac{15}{32} + \frac{4}{5}(1 - 1/2^{12})]\, n < \frac{3}{4}n - 4$. Since $\operatorname{ind} x_3 \not\equiv 0 \bmod 4$, this implies $d_3 < 4$, a contradiction.

(8.10) If $d_2 = 6$, then $d_3 > 6$.

Proof. Assume $d_2 = d_3 = 6$. Then

$$\operatorname{ind} x_j = \tfrac{5}{6}n - \tfrac{1}{6}(2f(x_j) + 2f(x_j^2) + f(x_j^3))$$

for $j = 2, 3$. This yields

$$2 + \frac{n}{6} = \frac{f(x_1)}{2} + \frac{1}{3}[f(x_2) + f(x_2^2) + f(x_3) + f(x_3^2)]$$

$$+ \frac{1}{6}[f(x_2^3) + f(x_3^3)]. \qquad (*)$$

Note that $f(x_1) \equiv f(x_1^3) \equiv f(x_3^3) \equiv 0 \bmod 2^m$, where $m = [e/2] - 1$. Suppose first that $f(x_2) = 1$. Then $f(x_2^2) = 1$ also. Hence $f(x_3) + f(x_3^3) \equiv 4 \bmod 2^m$. If $f(x_3) = f(x_3^2) = 2$, then

$$\frac{n}{6} = \frac{f(x_1)}{2} + \frac{1}{6}[f(x_3^2) + f(x_3^3)].$$

Since $f(x_1) \leqslant n/8$, it follows that $f(x_1) = 0$ and $f(x_2^3) = f(x_3^3) = n/2$. However, since $f(x_2^2) = 1$, x_2^2 cannot commute with a transvection. Thus x_2^3 is not a transvection, whence $f(x_2^3) < n/2$, a contradiction.

So we can assume $f(x_1), f(x_2) \neq 1$. If $f(x_2) = 0$ then $f(x_2^3) = 0$. By reading $(*)$ mod 16, we see that

$$f(x_2^2) + f(x_3) + f(x_3^2) \equiv 6 \bmod 16.$$

This implies $f(x_3) \leqslant 2$. If $f(x_3) = 2$, then $f(x_2^2) = f(x_3^2) = 2$. Thus $n = 3f(x_1) + f(x_3^3)$, whence $f(x_1) = n/4$ and $e \leqslant 12$. If $f(x_3) = 1$, then

$f(x_3^2)=1$ and $f(x_2^2)=4$, and again $e\leqslant 12$. If $f(x_3)=0=f(x_3^2)$, no solution exists.

So now $f(x_2)$, $f(x_3)>1$. If neither is 2, then Σ ind $x_i\equiv 0 \bmod 4$. So assume $f(x_2)=2$. Thus $f(x_2^2)=2$ or 4. In the first case, $f(x_3)=2$ and so $f(x_3^2)\leqslant 4$. Then Σ ind $x_i\not\equiv 30 \bmod 32$. So $f(x_2^2)=4$. This yields

$$n=3f(x_1)+2f(x_3)+2f(x_3^2)+f(x_3^2)+f(x_3^3). \qquad (**)$$

Since $e\leqslant 2e_3$, $f(x_3)\leqslant\sqrt{n}$. Moreover as $f(x_1)\,f(x_3^2)\,f(x_3^3)\neq 0$, it follows that $f(x_1)$, $f(x_3^2)$, and $f(x_3^3)\geqslant\sqrt{n}$. Note that since $f(x_3^2)=4$, e is even. Thus $2f(x_3)+2f(x_3^2)$ is not divisible by $4\sqrt{n}$. This implies that the righthand side of $(**)$ is not divisible by $64\sqrt{n}$. Thus $n<64\sqrt{n}$, whence $e<12$.

(8.11) $d_2\neq 6$.

Proof. Assume $(d_1, d_2)=(2, 6)$ and so by (8.10), $d_3>6$. Now $e_1\geqslant 3$ and $e_2\geqslant 9$ imply that ind $x_1>\frac{7}{16}n$ and ind $x_2\geqslant(3/4-1/2^9)\,n$. Thus ind $x_3<\frac{7}{8}n$, and so $d_3=7$, 8, 10, or 14. If $d_3=7$, then $e_3\geqslant 9$ implies ind $x_3\geqslant\frac{6}{7}(1-(1/2^9))n$ and Σ ind $x_i>2n$. If $d_3=8$, then $e_3\geqslant 9$ implies ind $x_3\geqslant(25/32-(1/2^{10}))n$. Also ind $x_3\equiv 0 \bmod 4$, and so ind $x_2\geqslant\frac{3}{4}n-2$. Thus ind $x_1<\frac{31}{64}n$ and so ind $x_1\leqslant\frac{15}{32}n$ and $e_1\leqslant 4$. Thus $e_j>12$ for $j=2, 3$. Thus ind $x_3\geqslant\frac{13}{16}n-72$, whence as above $e_1\leqslant 3$. Thus $e_j\geqslant n-3$ for $j=2, 3$. Then ind $x_3\geqslant\frac{27}{32}n-20$ and Σ ind $x_i>2n$. Similarly, if $d_3=10$, then ind $x_3\equiv 0 \bmod 4$. Hence ind $x_2\geqslant\frac{3}{4}n-2$. Since $e_3\geqslant 9$, this implies Σ ind $x_j>2n$. Essentially the same argument prevails when $d_3=12$ or 14.

THEOREM 8.12. *There are no examples with* $e>16$.

Proof. By previous results, we can assume $d_1=2$ and $6<d_2\leqslant d_3$. Since $e_2, e_3\geqslant 9$, it follows that ind $x_j\geqslant(\frac{5}{6}-\frac{3}{128})n$ for $j=2, 3$. Thus ind $x_1<\frac{7}{16}n$, and so $e_1\leqslant 2$. If $e_1=1$, then $d_2, d_3\geqslant 17$ and so ind $x_j\geqslant\frac{7}{8}n$ for $j=2, 3$. Hence Σ ind $x_i\geqslant 2n$. So assume $e_1=2$. Thus ind $x_1=\frac{3}{8}n$ and so $e_j\geqslant e-2$ for $j=2, 3$. This also implies $d_2, d_3>8$. As in (8.11), if $d_j\neq 12$, then ind $x_j>\frac{13}{16}n$ and Σ ind $x_i>2n$. Indeed, one sees that for $j>1$ if $d_j\neq 12$, then as $e_j\geqslant e-2\geqslant 15$, ind $x_j\geqslant\frac{17}{20}n-8$, while if $d_j=12$,

$$\begin{aligned}\text{ind } x_j&=\frac{11}{12}n-\frac{1}{12}\left[4f(x_j)+2f(x_j^2)+2f(x_j^3)+2f(x_j^4)+f(x_j^6)\right]\\&\geqslant\frac{11}{12}n-\frac{1}{12}\left[16+32+\frac{n}{2}+512+\frac{n}{2}\right]\\&=\frac{5}{6}n-\frac{140}{3}.\end{aligned}$$

Thus Σ ind $x_i\geqslant\frac{3}{8}n+\frac{5}{6}n-\frac{280}{3}>2n$.

9. The Case $F(G) = 1$

Throughout we assume G is a primitive group on Ω with $|\Omega| = n$. Let H be a point stabilizer. We assume $F^*(G)$ is nonabelian. So we can choose a simple component L. Set $\Delta = \{L = L_1, ..., L_t\}$ the set of G conjugates of L and $Q = L_1 \times \cdots \times L_t$. Suppose $G = \langle x_1, ..., x_r \rangle$ with $x_1 \cdots x_r = 1$. We also assume that $H \cap Q = H_1 \times \cdots \times H_t$, where $H_i = H \cap L_i$ (for if this fails, Theorem C2 applies). Thus $n = [Q : H \cap Q] = l^t$, where $l = [L : H \cap L]$. Note $l \geqslant 5$.

We need to obtain upper bounds for $f(x)$. Of course, if x is not a conjugate of H, $f(x) = 0$. So in computing these bounds we can always assume $x \in H$. As an H-set, $\Omega \cong \Omega_1 \times \cdots \times \Omega_t$, where $\Omega_i = L_i/H_i$ and $x \in H$ acts via

$$x : y(H \cap Q) \to xyx^{-1}(H \cap Q)$$

for $y \in Q$.

The next result is trivial but fundamental.

(9.1) If $x \in G$, then $f(x) \leqslant l^{m(x)}$, where $m(x)$ is the number of orbits of x on Δ.

Proof. We can assume $x \in H$. The proof reduces to the case of a single orbit. Here it is easy to see for $\omega_1 \in \Omega_1$, there is at most one fixed point of x with ω_1 as the first coordinate.

With (9.1) at our disposal, we can obtain lower bounds for $\mathrm{ind}(x)$. If the order of x is d, we use the formula $\mathrm{orb}(x) = (1/d) \sum_{i=1}^{d} f(x^i)$, whence $\mathrm{ind}(x) = n - (1/d) \sum_{i=1}^{d} f(x^i)$. This and (9.1) yield

(9.2) Suppose $x \in G$ and x acts as a permutation of order $d > 1$ on Δ. Then

(a) $\mathrm{ind}(x) \geqslant \left(\frac{d-1}{d}\right)\left(\frac{l-1}{l}\right) n \geqslant \frac{2}{5} n.$

(b) If $2 \neq d$ is prime, $\mathrm{ind}\, x \geqslant \left(\frac{d-1}{d}\right)\left(\frac{l^{d-1}-1}{l^{d-1}}\right) n \geqslant \frac{16}{25} n.$

(c) If $d = 4$, $\mathrm{ind}\, x \geqslant \left(\frac{3}{4} - \frac{2+l}{4l^3}\right) m \geqslant \frac{92}{125} n.$

(d) If $d = 6$, $\mathrm{ind}\, x \geqslant \left(\frac{5}{6} - \frac{2+2l+l^2}{6l^3}\right) n \geqslant \frac{98}{125} n.$

(e) If $d = 8$, $\mathrm{ind}\, x \geqslant \left(\frac{7}{8} - \frac{4+2l+l^3}{8l^7}\right) n > \frac{107}{125} n.$

(f) If $d=9$, $\operatorname{ind} x \geqslant \left(\frac{8}{9}-\frac{6+2l^3}{9l^8}\right)n > \frac{107}{125}n$.

(g) If $d=10$, $\operatorname{ind} x \geqslant \left(\frac{9}{10}-\frac{4+4l+l^4}{10l^5}\right)n > \frac{106}{125}n$.

(h) If $d=12$, $\operatorname{ind} x \geqslant \left(\frac{4}{12}-\frac{8+2l^2+3l^3}{12l^5}\right)n > \frac{107}{125}n$.

(i) If $d=15$, $\operatorname{ind} x \geqslant \left(\frac{14}{15}-\frac{8+4l^2+2l^4}{15l^6}\right)n > \frac{107}{125}n$.

(j) If $d=25$, $\operatorname{ind} x \geqslant \left(\frac{24}{25}-\frac{20+4l^4}{25l^{24}}\right)n > \frac{107}{125}n$.

(k) If $d=2$ and x does not act as a transposition on Δ, $\operatorname{ind} x \geqslant \left(\frac{1}{2}-\frac{1}{2l^2}\right)n$.

(l) If $d=3$ and x does not as a 3-cycle on Δ, $\operatorname{ind} x \geqslant \left(\frac{2}{3}-\frac{2}{3l^4}\right)n$.

Let d_i be the order of x_i and d_i' the order of x_i as a permutation on Δ. By reordering, we can assume $d_1' \leqslant \cdots \leqslant d_s'$ (possibly $s=0$) and $d_i'=1$ for $i>s$.

THEOREM 9.3. *Let K be the kernel of $G \to \operatorname{Sym}(\Delta)$. One of the following holds*:

(a) $s=0$ (so $\Delta=\{L\}$ *and* $G=K$).

(b) $s=2$ (*so G/K is cyclic*).

(c) $s=3$ *and* (d_1', d_2', d_3') *is one of the following*:

(i) $(2,4,4)$, $(2,3,6)$, or $(3,3,3)$ *with* $(G/K)''=1$

(ii) $(2,2,m)$ *with G/K dihedral,*

(iii) $(2,3,m)$, $m \leqslant 5$, *with* $G/K=A_4$, S_4, *or* A_5, *or*

(iv) $(2,4,5)$ *with* $G/K=S_5$, $t=5$, *and* $l \leqslant 9$.

(v) $(2,4,6)$ *with* $G/K=S_5$ *and* $t=l=5$.

(d) $s=4$ *and* $(d_1', d_2', d_3'\ d_4')$ *is either*

(i) $(2,2,2,2)$ *and* $(G/K)''=1$,

(ii) $(2,2,2,3)$, $t=4$, $l \leqslant 7$, *and* $G/K=S_4$, *or*

(iii) $(2,2,2,4)$, $t=4$, $l \leqslant 6$, *and* $G/K=S_4$.

(e) $\Sigma \operatorname{ind} x_i \geqslant (2+\varepsilon)n$, *where* $\varepsilon = 1/1000$.

Proof. Assume (e) does not hold. By (9.1) ind $x_i \geqslant \frac{2}{5}n$ for $1 \leqslant i \leqslant s$. Thus $s < 6$. If $s = 5$, then (9.1) implies each $d_1' = 2$ or (e) holds. Moreover, if x_i does not act as a transposition on Δ, ind $x_i \geqslant \frac{12}{25}n$, and (e) holds. Since the product of five transpositions is non-trivial, $s \neq 5$. If $s \leqslant 2$, the result holds. So we first consider $s = 4$.

If two of the d_i' are bigger than 2, $\sum_{i=1}^{s}$ ind $x_i \geqslant (2 \cdot \frac{2}{5} + 2 \cdot \frac{16}{25}) > (2+\varepsilon)n$. So $(d_1', d_2', d_3', d_4') = (2, 2, 2, m)$. If none of the x_i are transpositions, then (9.1) and (9.2) imply Σ ind $x_i \geqslant (3 \cdot (\frac{12}{25}) + (\frac{16}{25}))n > (2+\varepsilon)n$. If only x_1 is a transposition, a similar computation shows Σ ind $x_i > (2+\varepsilon)n$ unless x_2 and x_3 are products of two transpositions and x_4, is a 3-cycle, a contradiction as $x_1 \cdots x_4 \in K$. So we may assume x_1 and x_2 act as transpositions. Since $G = \langle x_1, x_2, x_3 \rangle K$, this implies $t = |\Delta| \leqslant 6$. This leaves the following possibilities:

(a) $t = 6$, x_3 a product of 3 transpositions, x_4 a 6-cycle.

(b) $t = 5$, x_3 a product of 2 transpositions, x_4 a 5-cycle.

(c) $t = 4$.

(d) $t \leqslant 3$.

If (d) holds, then $m = 2$ and case (d i) of the theorem holds. If (a) or (b) holds, then Σ ind $x_i > (2+\varepsilon)n$ by (9.1) and (9.2).

So we are left to consider (c). There are two subcases. The first is if x_1, x_2, and x_3 are transpositions (and so x_4 is a 4-cycle). The second is if x_3 is not a transposition and x_4 is a 3-cycle. In the first case either (e) holds or

$$(2+\varepsilon)n \geqslant \sum_{i=1}^{4} \text{ind } x_i \geqslant \left(\frac{3}{2} - \frac{3}{2l} + \frac{3}{4} - \frac{2+l}{4l^3}\right)$$
$$= 2n + \left(\frac{1}{4} - \frac{6l^2 + l + 2}{4l^3}\right)n,$$

whence $l = 5$ or 6. Similarly, in the second case,

$$(2+\varepsilon)n \geqslant \sum_{i=1}^{4} \text{ind } x_i \geqslant \left(\left(1 - \frac{1}{l}\right) + \left(\frac{1}{2} - \frac{1}{2l^2}\right) + \left(\frac{2}{3} - \frac{2}{3l^2}\right)\right)n$$
$$= 2n + \left(\frac{1}{6} - \frac{6l+7}{6l^2}\right)n,$$

whence $l \leqslant 6$.

If $d_1' = d_2' = d_3' = d_4' = 2$, then by Proposition 2.4, $G'' = 1$. So the theorem holds.

Now assume $s = 3$. If $\Sigma(1/d_i') \geqslant 1$, then Proposition 2.4 implies that (ci), (cii), or (ciii) holds. So $\Sigma(1/d_i') < 1$. Recall $d_1' \leqslant d_2' \leqslant d_3'$. If $d_1' > 2$, then

$d_3' > 3$. Then (9.2) implies $\sum_{i=1}^{3} \text{ind } x_i > (2+\varepsilon)n$. So $d_1' = 2$ and $d_2' > 2$. If x_1 is a transposition, then as $\langle x_1, x_2 \rangle$ acts transitively on Δ, x_2 is a $(t-1)$-cycle and x_3 is a t-cycle. By (9.2) and Σ ind $x_i < (2+\varepsilon)n$, this yields $t \leqslant 5$.

If $t < 5$, there is nothing to prove.If $t = 5$, the action of G on Δ must be S_5 (as it is primitive and contains a transposition). Moreover,

$$(2+\varepsilon)n \geqslant \sum_{i=1}^{3} \text{ind}(x_i) \geqslant \left(\frac{1}{2} - \frac{1}{2l} + \frac{3}{4} - \frac{2+l}{4l^3} + \frac{4}{5} - \frac{4}{5l^4}\right)n$$

$$= 2n + \frac{n}{20}\left(1 - \frac{10l^3 + 10l + 5l^2 + 16}{l^4}\right).$$

Thus $l \leqslant 10$.

Hence $d_1' = 2$ and x_1 is not a transposition. Thus ind $x_1 \geqslant \frac{12}{25}n$. If $d_2' = 3$, then $d_3' \geqslant 7$. Thus x_2 is not a 3-cycle. Hence ind $x_2 \geqslant \frac{416}{625}n$ by (9.1). Also by (9.1), ind $x_3 > \frac{107}{125}n$. Thus Σ ind $x_i > (2+\varepsilon)n$. Finally, if $d_2' \geqslant 4$, $d_3' \geqslant 5$, then by (9.2), Σ ind $x_i > (2+\varepsilon)n$ unless $d_2' = 4$, $d_3' = 6$, and $l = 5$. Moreover, by (9.1), Σ ind $x_i > (2+\varepsilon)n$ unless x_1 is a product of two transposition, x_2 is a 4-cycle, and x_3 is the product of a transposition and a 3-cycle. Thus $t = 5$, $G/K = S_5$, and (cv) holds. This concludes the proof.

Now Theorem D follows for $K/F^*(G)$ embeds in a direct product of $\text{Out}(L) \times \cdots \times \text{Out } L$ which is solvable by the Schreier conjecture. We now prove Theorem C1.

COROLLARY 9.4. *$H \cap F^*(G) \neq 1$ if G is primitive of genus zero and $F(G) = 1$.*

Proof. By [AS] if $H \cap F^*(G) = 1$, the point stabilizer of L in the action of H on Δ must induce the full group of inner automorphisms on L. By (9.3), this point stabilizer is solvable.

We now prove Theorem E. So assume L is a component of G and that whenever $L = F^*(M)$ and $T \leqslant M$ with $T \not\trianglelefteq L$, then for $1 \neq x \in M$, $|x^M \cap T|/|x^M| \leqslant \frac{1}{85}$. In particular L has no subgroup of index smaller than 85.

First assume $H \cap Q = 1$. Then as an H-set, $\Omega = Q$, and H acts via conjugation. Hence if $x \in H$, $f(x) = |C_Q(x)|$. Since L has no proper subgroup of index less than 85 neither does Q. Hence $f(x) \leqslant \frac{1}{85}n$ for any $x \neq 1$ (as $C_H(Q) = 1$).

Now assume $H \cap Q \neq 1$. By Theorem D and [AS], $H \cap L \neq 1$ and $F^*(G) = Q$. By the hypothesis, $l \geqslant 85$. Hence by (9.1) if x acts nontrivially on Δ, then $f(x) \leqslant (1/l)n \leqslant (1/85)n$. So we must consider $x \in K$. Since $F^*(G) = Q$, $G \leqslant \text{Aut } Q$, $Q \leqslant K \leqslant \text{Aut } L_1 \times \cdots \times \text{Aut } L_t$. Thus we can write $x = (x_1, ..., x_t)$, $x_i \in \text{Aut } L_i$ (note x_i need not be in G but is in Aut Q). As usual, we can also assume that $x \in H$. Thus x_i normalizes H_i. Now

$f(x)=f_1(x_1)\cdots f_t(x_t)$, where $f_i(x_i)$ is the number of fixed points of x_i on $L_i\langle x_i\rangle/H_i\langle x_i\rangle$. By hypothesis, if $x_i\neq 1$,

$$f_i(x_i)=\frac{|x_i^{L_i}\cap H_i\langle x_i\rangle|}{|x_i^{L_i}|}\leqslant\frac{1}{85}l.$$

Since some $x_i\neq 1$, $f(x)\leqslant\frac{1}{85}n$.

So we have shown:

(9.5) If $1\neq x\in G$, $f(x)\leqslant\frac{1}{85}n$.

Since $\operatorname{ind} x=n-(1/d)\sum_{i=1}^{d}f(x^i)$, where d is the order of x, this implies $\operatorname{ind} x\geqslant((d-1)/d\ \frac{84}{85}n$. Now $G=\langle x_1,\ldots,x_r\rangle$ with $x_1\cdots x_r=1$ and $\Sigma\ \operatorname{ind} x_i=2n-2$. Recall d_i is the order of x_i. Now (9.5) yields

(9.6) One of the following holds:

(i) $r=4$, $(d_1,d_2,d_3,d_4)=(2,2,2,2)$.

(ii) $r=3$ and $\Sigma\,(1/d_i)\geqslant 1$.

(iii) $r\leqslant 2$.

However, in all these cases G is either solvable or isomorphic to A_5. This is obviously not possible and concludes the proof.

One can prove in a similar manner (as indeed Shih [S] has) that $H\cap Q\neq 1$ in all cases, whence except for those described in [A], $H\cap L\neq 1$.

The next result shows that $L_2(p)$, for p large, cannot be a component of a primitive genus zero group.

THEOREM 9.7. *Let $F^*(G)=L\cong L_2(p)$, p prime. Then for $T<G$ with $T\not\geqslant L$ and $1\neq x\in G$,*

$$\frac{|x^G\cap T|}{|x^G|}\leqslant\frac{4}{p-1}.$$

Proof. If $p<7$, there is nothing to prove. So assume $p>5$. Set $H=T\cap L$. By [S, p. 412], H is contained in some maximal subgroup M of L, where

(a) $M\cong A_4$ or A_5 or S_4

(b) M is a Borel subgroup, or

(c) M is a maximal torus (so M is dihedral of order $p\pm 1$).

If $x\in L$, then it is easy to calculate that $|x^L|\geqslant p(p-1)/2$. Also, $|x^G\cap M|\leqslant 15$, $2p$, or $(p+1)/2$ in each corresponding case. Thus

$$\frac{|x^G\cap T|}{|x^G|}\leqslant\frac{|x^G\cap M|}{|x^G|}\leqslant\frac{4p}{p(p-1)}=\frac{4}{p-1},$$

for $1\neq x\in L$.

Since we can assume that x has prime order, it suffices only to consider the case x is involution not in L. The $|C_G(x)| \leqslant 2(p+1)$. Hence $|x^G| \geqslant p(p-1)/2$. Also note that $|x^G \cap T|$ is at most the number of involutions in xH. Thus in case (a), $|x^G \cap T| \leqslant 10$, and in case (c), $|x^G \cap T| \leqslant |H| \leqslant p+1$. Thus we can assume H is contained in a Borel subgroup M of L. Since two distinct Borel subgroups intersect in a torus, M is unique. Thus $M^x = M$. One then computes that the number of involutions in xM is $2p$. Thus, as above, the desired inequality holds.

A similar argument (considering a few extra cases) will yield the same type of bound for $L_2(q)$. We conjecture that if L is any Chevalley group defined over the field of q elements, then the desired ratio tends to zero as q tends to infinity. The results in [L, LS] should be useful in this problem.

Now Corollary F follows. For suppose $L_2(p)$, $p > 341$ is a composition factor of a genus zero group G. By Corollary 2.2, we can assume G is a primitive genus zero group. By Theorems 9.7, C2, D, and E, $F^*(G)$ is abelian. Finally, by Theorem A, as $L_2(p)$, $p > 341$, is not as a composition factor of a subgroup of $GL_6(3)$, $SL_{16}(2)$, or $GL_2(r)$, $r \leqslant 11$, the result holds.

REFERENCES

[A] M. ASCHBACHER, On conjectures of Guralnick and Thompson, *J. Algebra*, in press.

[AS] M. ASCHBACHER AND L. SCOTT, Maximal subgroups of finite groups, *J. Algebra* **92** (1985), 44–80.

[FLS] W. FEIT, R. C. LYNDON, AND L. L. SCOTT, A remark about permutations, *J. Combin. Theory Ser. A* **18** (1975), 234–235.

[Fr] M. FRIED, Galois groups and complex multiplication, *Trans. Amer. Math. Soc.* **237** (1978), 141–162.

[FG] M. FRIED AND R. GURALNICK, The generic curve of genus $g > 6$ is not uniformized by radicals, preprint.

[H] B. HUPPERT, "Endliche Gruppen I," Springer-Verlag, Berlin, 1967.

[L] M. LIEBECK, On the orders of the maximal subgroups of the finite classical groups, *Proc. London Math. Soc.* (3) **50** (1985), 426–446.

[LS] M. LIEBECK AND J. SAXL, On the orders of maximal subgroups of the finite exceptional groups of Lie type, *Proc. London Math. Soc.* (3) **55** (1987), 299–330.

[M] W. MAGNUS, "Noneuclidean Tesselations and Their Groups," Academic Press, New York, 1974.

[Mc] J. MCLAUGHLIN, Some subgroups of $SL_n(F_2)$, *Illinois J. Math* **13** (1969), 108–115.

[N] M. NEUBAUER, "On Solvable Monodromy Groups of Fixed Genus," Ph.D. Thesis, University of Southern California, 1989.

[S] T. SHIH, A note on groups of genus zero, preprint.

[Z] O. ZARISKI, "Collected Papers, Vol. III," MIT Press, Cambridge, MA, 1978.